

T S3/5/1

3/5/1

DIALOG(R)File 351:Derwent WPI

(c) 2005 Thomson Derwent. All rts. reserv.

013608276

WPI Acc No: 2001-092484/200111

XRPX Acc No: N01-069981

**Electronic storage device for guaranteeing originality of electronic data
varies level of access based on if data are original data or not**

Patent Assignee: RICOH KK (RICO)

Inventor: KANAI Y; YACHIDA M

Number of Countries: 002 Number of Patents: 007

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
DE 10024753	A1	20001221	DE 1024753	A	20000519	200111 B
JP 2000339223	A	20001208	JP 99145340	A	19990525	200113
JP 2001005728	A	20010112	JP 99173371	A	19990618	200118
JP 2001147898	A	20010529	JP 99328802	A	19991118	200136
JP 2001154577	A	20010608	JP 99338741	A	19991129	200138
JP 2001209582	A	20010803	JP 200015092	A	20000124	200150
JP 2001209581	A	20010803	JP 200015091	A	20000124	200150

Priority Applications (No Type Date): JP 200015092 A 20000124; JP 99145340
A 19990525; JP 99173371 A 19990618; JP 99328802 A 19991118; JP 99338741 A
19991129; JP 200015091 A 20000124

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 10024753	A1	159		G06F-012/14	
JP 2000339223	A	29		G06F-012/14	
JP 2001005728	A	46		G06F-012/14	
JP 2001147898	A	11		G06F-015/00	
JP 2001154577	A	12		G09C-001/00	
JP 2001209582	A	18		G06F-012/14	
JP 2001209581	A	16		G06F-012/14	

Abstract (Basic): DE 10024753 A1

NOVELTY - The storage device includes a storage unit which stores electronic data consisting of a number of content files as a single original in an identifiable state. An access unit controls the access to the original electronic data at a level which is different from the level of access to non-original electronic data. The storage unit stores tamper detection information as original information corresponding to the electronic data.

DETAILED DESCRIPTION - The storage device may include a tamper detection information computing device which receives a request to re-store the electronic data as a single original using an encryption key to compute tamper detection information for each of the content files. A second tamper detection information computing device uses the encryption key to compute second tamper detection information for edition management information. **INDEPENDENT CLAIMS** are included for an electronic storage device, an authorization verification system, an electronic storage method, an authorization verification method, damage recovery method and a storage medium for storing a program in a computer.

USE - For originality-guarantee electronic preservation systems using large-capacity storage media.

ADVANTAGE - Allows the originality of a combined document comprising multiple files to be guaranteed.

pp; 159 DwgNo 0/74
Title Terms: ELECTRONIC; STORAGE; DEVICE; GUARANTEE; ELECTRONIC; DATA; VARY
; LEVEL; ACCESS; BASED; DATA; ORIGINAL; DATA
Derwent Class: P85; T01
International Patent Class (Main): G06F-012/14; G06F-015/00
International Patent Class (Additional): G06F-003/06; G06F-009/06;
G06F-012/00; G06F-012/16; G06F-017/30; G06F-017/60; G09C-001/00
File Segment: EPI; EngPI
?

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-5728
(P2001-5728A)

(43) 公開日 平成13年1月12日 (2001.1.12)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 Z 5 B 0 1 7
12/00	5 2 0	12/00	5 2 0 E 5 B 0 4 9
	5 3 7		5 3 7 A 5 B 0 7 5
17/60		15/21	Z 5 B 0 8 2
17/30		15/40	3 2 0 B
審査請求 未請求 請求項の数15 O L (全 46 頁) 最終頁に続く			

(21) 出願番号 特願平11-173371

(22) 出願日 平成11年6月18日 (1999.6.18)

(71) 出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(72) 発明者 金井 洋一

東京都大田区中馬込1丁目3番6号 株式会社リコー内

(72) 発明者 谷内田 益義

東京都大田区中馬込1丁目3番6号 株式会社リコー内

(74) 代理人 100089118

弁理士 酒井 宏明

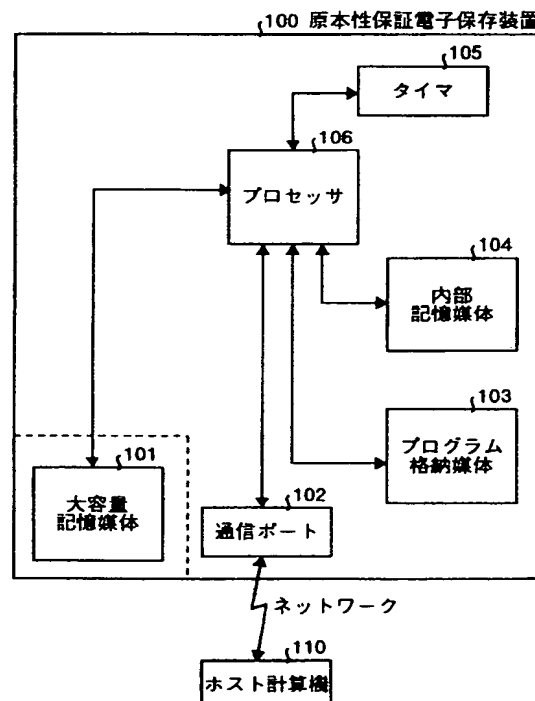
最終頁に続く

(54) 【発明の名称】 原本性保証電子保存装置、原本性保証電子保存方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 複数のファイルから形成される複合文書の原本性を効率良く保証することができる原本性保証電子保存方法および記録媒体を提供すること。

【解決手段】 複数のコンテンツファイルにより形成される電子データを一つの原本として大容量記憶媒体101に保存しておき、プロセッサ106がこの大容量記憶媒体101の電子データをアクセスするに際しては、原本とそうでないものとでアクセス制御のレベルを変える。



【特許請求の範囲】

【請求項 1】 所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存装置において、複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存する保存手段と、

前記保存工程によって保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうアクセス制御手段と、を備えたことを特徴とする原本性保証電子保存装置。

【請求項 2】 前記保存手段は、前記電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに前記記憶部に保存することを特徴とする請求項 1 に記載の原本性保証電子保存装置。

【請求項 3】 前記保存手段は、前記電子データに対応する第 1 の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第 2 の改ざん検知情報を算定し、算定した第 2 の改ざん検知情報を前記属性情報とともに前記記憶部に保存することを特徴とする請求項 1 に記載の原本性保証電子保存装置。

【請求項 4】 前記保存手段は、前記複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第 1 の改ざん検知情報をそれぞれ算定する第 1 の改ざん検知情報算定手段と、

前記第 1 の改ざん検知情報算定手段により算定された第 1 の改ざん検知情報を含む版管理情報を作成する版管理情報作成手段と、

前記版管理情報作成手段により作成された版管理情報に係る第 2 の改ざん検知情報を前記暗号鍵を用いて算定する第 2 の改ざん検知情報算定手段と、

前記第 2 の改ざん検知情報算定手段により算定された第 2 の改ざん検知情報を含む属性情報に係る第 3 の改ざん検知情報を前記暗号鍵を用いて算定する第 3 の改ざん検知情報算定手段と、

前記第 3 の改ざん検知情報算定手段により算定された第 3 の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加手段と、

前記エントリ追加手段によりエントリが追加されたデータリストに係る第 4 の改ざん検知情報を前記暗号鍵を用いて算定する第 4 の改ざん検知情報算定手段と、

前記第 4 の改ざん検知情報算定手段により算定された第 4 の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納手段と、

を備えたことを特徴とする請求項 1 に記載の原本性保証電子保存装置。

【請求項 5】 前記アクセス制御手段は、外部から原本となるコンテンツファイルの読み出し要求

を受け付けた際に、前記記憶部から第 4 の改ざん検知情報および前記データリストを読み出す読み出し手段と、前記読み出し手段により読み出された第 4 の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第 1 の改ざん検知手段と、

前記データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、取り出したエントリに含まれる第 3 の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第 2 の改ざん検知手段と、

前記記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第 2 の改ざん検知情報および前記復号鍵を用いて前記版管理情報の改ざん検知をおこなう第 3 の改ざん検知手段と、

前記版管理情報から読み出し対象となるコンテンツファイルに係る第 1 の改ざん検知情報を取り出し、該第 1 の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第 4 の改ざん検知手段と、

前記コンテンツファイルが改ざんされていない場合に、前記記憶部に記憶したコンテンツファイルを要求元に提供する提供手段と、

を備えたことを特徴とする請求項 4 に記載の原本性保証電子保存装置。

【請求項 6】 前記アクセス制御手段は、外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、前記記憶部から第 4 の改ざん検知情報およびデータリストを読み出す読み出し手段と、

前記読み出し手段により読み出された第 4 の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第 1 の改ざん検知手段と、

前記データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第 3 の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第 2 の改ざん検知手段と、

前記暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第 1 の改ざん検知情報をそれぞれ算定する第 1 の改ざん検知情報算定手段と、

前記第 2 の改ざん検知情報算定手段により算定された第 2 の改ざん検知情報を含む属性情報に係る第 3 の改ざん検知情報を前記暗号鍵を用いて算定する第 3 の改ざん検知情報算定手段と、

前記第 3 の改ざん検知情報算定手段により算定された第 3 の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加手段と、

前記エントリ追加手段によりエントリが追加されたデータリストに係る第4の改ざん検知情報を前記暗号鍵を用いて算定する第4の改ざん検知情報算定手段と、
前記第4の改ざん検知情報算定手段により算定された第4の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納手段と、
を備えたことを特徴とする請求項4に記載の原本性保証電子保存装置。

【請求項7】 前記アクセス制御手段は、
外部から原本となる電子データの版を指定した複製要求を受け付けた際に、前記第4の改ざん検知情報およびデータリストを読み出す読み出し手段と、
前記読み出し手段により読み出された第4の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第1の改ざん検知手段と、前記データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第2の改ざん検知手段と、
前記属性情報から複製対象となる版に係る第2の改ざん検知情報を取り出し、該第2の改ざん検知情報および前記復号鍵を用いて版管理情報の改ざん検知をおこなう第3の改ざん検知手段と、
前記版管理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該第1の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第4の改ざん検知手段と、
前記記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製する複製手段と、
前記複製手段により複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更する属性変更手段と、
前記属性変更手段により変更された属性コードを含む属性情報および前記暗号鍵を用いて第3の改ざん検知情報を再算定する第3の改ざん検知情報再算定手段と、
前記第3の改ざん検知情報再算定手段により算定された第3の改ざん検知情報を含むエントリにより前記データリストを更新し、更新後のデータリストに係る第4の改ざん検知情報を前記暗号鍵を用いて再算定する第4の改ざん検知情報再算定手段と、
を備えたことを特徴とする請求項4に記載の原本性保証電子保存装置。

【請求項8】 所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存方法において、
複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存する保存工程と、
前記保存工程によって保存した原本の電子データと該原

本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうアクセス制御工程と、
を含んだことを特徴とする原本性保証電子保存方法。

【請求項9】 前記保存工程は、前記電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに前記記憶部に保存することを特徴とする請求項8に記載の原本性保証電子保存方法。

【請求項10】 前記保存工程は、前記電子データに対応する第1の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第2の改ざん検知情報を算定し、算定した第2の改ざん検知情報を前記属性情報とともに前記記憶部に保存することを特徴とする請求項8に記載の原本性保証電子保存方法。

【請求項11】 前記保存工程は、
前記複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第1の改ざん検知情報をそれぞれ算定する第1の改ざん検知情報算定工程と、
前記第1の改ざん検知情報算定工程により算定された第1の改ざん検知情報を含む版管理情報を作成する版管理情報作成工程と、
前記版管理情報作成工程により作成された版管理情報に係る第2の改ざん検知情報を前記暗号鍵を用いて算定する第2の改ざん検知情報算定工程と、
前記第2の改ざん検知情報算定工程により算定された第2の改ざん検知情報を含む属性情報に係る第3の改ざん検知情報を前記暗号鍵を用いて算定する第3の改ざん検知情報算定工程と、
前記第3の改ざん検知情報算定工程により算定された第3の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加工程と、
前記エントリ追加工程によりエントリが追加されたデータリストに係る第4の改ざん検知情報を前記暗号鍵を用いて算定する第4の改ざん検知情報算定工程と、前記第4の改ざん検知情報算定工程により算定された第4の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納工程と、
を含んだことを特徴とする請求項8に記載の原本性保証電子保存方法。

【請求項12】 前記アクセス制御工程は、
外部から原本となるコンテンツファイルの読み出し要求を受け付けた際に、前記記憶部から第4の改ざん検知情報および前記データリストを読み出す読み出し工程と、
前記読み出し工程により読み出された第4の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第1の改ざん検知工程と、

前記データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、取り出したエントリに含まれる第3の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第2の改ざん検知工程と、

前記記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第2の改ざん検知情報および前記復号鍵を用いて前記版管理情報の改ざん検知をおこなう第3の改ざん検知工程と、

前記版管理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該第1の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第4の改ざん検知工程と、

前記コンテンツファイルが改ざんされていない場合に、前記記憶部に記憶したコンテンツファイルを要求元に提供する提供工程と、

を含んだことを特徴とする請求項11に記載の原本性保証電子保存方法。

【請求項13】 前記アクセス制御工程は、外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、前記記憶部から第4の改ざん検知情報およびデータリストを読み出す読み出し工程と、

前記読み出し工程により読み出された第4の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第1の改ざん検知工程と、

前記データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第2の改ざん検知工程と、前記暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第1の改ざん検知情報をそれぞれ算定する第1の改ざん検知情報算定工程と、

前記第2の改ざん検知情報算定工程により算定された第2の改ざん検知情報を含む属性情報に係る第3の改ざん検知情報を前記暗号鍵を用いて算定する第3の改ざん検知情報算定工程と、

前記第3の改ざん検知情報算定工程により算定された第3の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加工程と、

前記エントリ追加工程によりエントリが追加されたデータリストに係る第4の改ざん検知情報を前記暗号鍵を用いて算定する第4の改ざん検知情報算定工程と、

前記第4の改ざん検知情報算定工程により算定された第4の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納工程と、

を含んだことを特徴とする請求項11に記載の原本性保証電子保存方法。

【請求項14】 前記アクセス制御工程は、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、前記第4の改ざん検知情報およびデータリストを読み出す読み出し工程と、

前記読み出し工程により読み出された第4の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第1の改ざん検知工程と、前記データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第2の改ざん検知工程と、

前記属性情報から複製対象となる版に係る第2の改ざん検知情報を取り出し、該第2の改ざん検知情報および前記復号鍵を用いて版管理情報の改ざん検知をおこなう第3の改ざん検知工程と、

前記版管理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該第1の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第4の改ざん検知工程と、

前記記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製する複製工程と、

前記複製工程により複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更する属性変更工程と、

前記属性変更工程により変更された属性コードを含む属性情報および前記暗号鍵を用いて第3の改ざん検知情報を再算定する第3の改ざん検知情報再算定工程と、

前記第3の改ざん検知情報再算定工程により算定された第3の改ざん検知情報を含むエントリにより前記データリストを更新し、更新後のデータリストに係る第4の改ざん検知情報を前記暗号鍵を用いて再算定する第4の改ざん検知情報再算定工程と、

を含んだことを特徴とする請求項11に記載の原本性保証電子保存方法。

【請求項15】 前記請求項8～14のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存装置、原本性保証電子保存方法および記録媒体に関し、特に、複数のファイルから形成される複合文書の原本性を効率良く保証することができる原本性保証電子保存装置、原本性保証電子保存方法および記録媒体に關す

る。

【0002】

【従来の技術】近年のコンピュータ技術の進展に伴うペーパーレス化の進展に伴って、紙によって原本書類として保存されていた情報が電子データの形式で保存される場合が増えてきたため、かかる電子データの原本性を保証する従来技術が知られている。

【0003】たとえば、「金井他：原本性保証電子保存システムの開発—システムの構築—, Medical Imaging Technology, Vol.16, No.4, Proceedings of JAMIT Annual Meeting'98(1998)」や、「国分他：原本性保証電子保存システムの開発, (特) 情報処理振興事業協会発行 創造的ソフトウェア育成事業およびエレクトロニック・コマース推進事業 最終成果発表会論文集 創造的ソフトウェア育成事業編(1998)」には、電子データの原本性を保証するシステムの一例が開示されている。

【0004】かかる従来技術を用いると、電子データの原本性を保証することが可能となり、これにより原本書類を電子データの形式で保存し、もって高度情報化社会の推進並びに社会全体の生産性向上に寄与することができる。

【0005】

【発明が解決しようとする課題】しかしながら、これらの従来技術のものは、原本となる電子文書が1つのファイルで形成されることを前提としており、HTML、XMLおよびSGMLのように複数のファイルによって電子文書が形成される場合を考慮したものではないので、かかる複数のファイルによって形成される電子文書（以下「複合文書」と言う）の原本性を効率良く保証することができないという問題がある。

【0006】すなわち、従来技術を用いてかかる複合文書の原本性を保証するには、複数のファイルを一つのファイルにまとめた後に原本性保証電子保存装置に保存するか、または各ファイルをそれぞれ別個の原本として原本性保証電子保存装置に保存せざるを得ない。

【0007】しかし、複数のファイルを一つのファイルにまとめることとしたのでは、どこからどこまでがどのファイルに相当するデータであるかを外部アプリケーションプログラムなどによって管理しなければならないため、その管理負担が大きいという問題がある。また、一つの塊にまとめられたデータは特殊なフォーマットとなってしまうために、外部アプリケーションとして取り扱い難くなり、原本データの見読性が低下するという問題もある。

【0008】一方、各ファイルをそれぞれ別個の原本として保存することとしたのでは、各原本がもともと一つの文書を形成するにもかかわらず、各原本がそれぞれ別個に編集され、次第に各原本の相互関係が不明確になるおそれがある。

【0009】これらのことから、複数のファイルから形

成される複合文書の原本性を原本性保証電子保存装置においていかに効率良く保証するかが極めて重要な課題となっている。

【0010】この発明は、上記問題（課題）に鑑みてなされたものであり、複数のファイルから形成される複合文書の原本性を効率良く保証することができる原本性保証電子保存装置、原本性保証電子保存方法および記録媒体を提供することを目的とする。

【0011】

【課題を解決するための手段】上記目的を達成するために、請求項1の発明に係る原本性保証電子保存装置は、所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存方法において、複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存する保存手段と、前記保存手段によって保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうアクセス制御手段と、を備えたことを特徴とする。

【0012】この請求項1の発明によれば、複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存し、保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうこととしたので、複数のファイルから形成される複合文書の原本性を効率良く保証することができる。

【0013】また、請求項2の発明に係る原本性保証電子保存装置は、前記保存手段は、前記電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに前記記憶部に保存することを特徴とする。

【0014】この請求項2の発明によれば、電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに記憶部に保存することとしたので、効率良く改ざん検知をおこなうことができる。

【0015】また、請求項3の発明に係る原本性保証電子保存装置は、前記保存手段は、前記電子データに対応する第1の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第2の改ざん検知情報を算定し、算定した第2の改ざん検知情報を前記属性情報とともに前記記憶部に保存することを特徴とする。

【0016】この請求項3の発明によれば、電子データに対応する第1の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第2の改ざん検知情報を算定し、算定した第2の改ざん検知情報を属性情報とともに記憶部に保存することとしたので、電子データ並びにアクセス履歴を含む改ざんを効率良く検知することができる。

【0017】また、請求項4の発明に係る原本性保証電

子保存装置は、前記保存手段は、前記複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第1の改ざん検知情報をそれぞれ算定する第1の改ざん検知情報算定手段と、前記第1の改ざん検知情報算定手段により算定された第1の改ざん検知情報を含む版管理情報を作成する版管理情報作成手段と、前記版管理情報作成手段により作成された版管理情報に係る第2の改ざん検知情報を前記暗号鍵を用いて算定する第2の改ざん検知情報算定手段と、前記第2の改ざん検知情報算定手段により算定された第2の改ざん検知情報を含む属性情報に係る第3の改ざん検知情報を前記暗号鍵を用いて算定する第3の改ざん検知情報算定手段と、前記第3の改ざん検知情報算定手段により算定された第3の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加手段と、前記エントリ追加手段によりエントリが追加されたデータリストに係る第4の改ざん検知情報を前記暗号鍵を用いて算定する第4の改ざん検知情報算定手段と、前記第4の改ざん検知情報算定手段により算定された第4の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納手段と、を備えたことを特徴とする。

【0018】この請求項4の発明によれば、複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第1の改ざん検知情報をそれぞれ算定し、算定した第1の改ざん検知情報を含む版管理情報を作成して第2の改ざん検知情報を算定し、算定した第2の改ざん検知情報を含む属性情報に係る第3の改ざん検知情報を算定し、算定した第3の改ざん検知情報を含むデータエントリを作成して記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第4の改ざん検知情報を算定し、算定した第4の改ざん検知情報と複数のコンテンツとを記憶部に格納することとしたので、複数のコンテンツファイルからなる新規データを改ざん防止措置を施しつつ効率良く格納することができる。

【0019】また、請求項5の発明に係る原本性保証電子保存装置は、前記アクセス制御手段は、外部から原本となるコンテンツファイルの読み出し要求を受け付けた際に、前記記憶部から第4の改ざん検知情報および前記データリストを読み出す読み出し手段と、前記読み出し手段により読み出された第4の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第1の改ざん検知手段と、前記データリストから読み出し対象となるコンテンツファイル

に含まれる第3の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第2の改ざん検知手段と、前記記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第2の改ざん検知情報および前記復号鍵を用いて前記版管理情報の改ざん検知をおこなう第3の改ざん検知手段と、前記版管理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該第1の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第4の改ざん検知手段と、前記コンテンツファイルが改ざんされていない場合に、前記記憶部に記憶したコンテンツファイルを要求元に提供する提供手段と、を備えたことを特徴とする。

【0020】この請求項5の発明によれば、外部から原本となるコンテンツファイルの読み出し要求を受け付けた際に、記憶部から第4の改ざん検知情報およびデータリストを読み出し、読み出した第4の改ざん検知情報および復号鍵を用いてデータリストの改ざん検知をおこない、データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、このエントリに含まれる第3の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第2の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該第1の改ざん検知情報および復号鍵を用いてコンテンツファイルの改ざん検知をおこない、コンテンツファイルが改ざんされていない場合に、記憶部に記憶したコンテンツファイルを要求元に提供することとしたので、多段階に渡って改ざんを防止しつつコンテンツファイルの読み出しを効率良くおこなうことができる。

【0021】また、請求項6の発明に係る原本性保証電子保存装置は、前記アクセス制御手段は、外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、前記記憶部から第4の改ざん検知情報およびデータリストを読み出す読み出し手段と、前記読み出し手段により読み出された第4の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第1の改ざん検知手段と、前記データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第2の改ざん検知手段と、前記暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第1の改ざん検知情報をそれぞれ算定する第1の改ざん検知情報算定手段と、前記第2の改ざん検知情報算定手

段により算定された第2の改ざん検知情報を含む属性情報に係る第3の改ざん検知情報を前記暗号鍵を用いて算定する第3の改ざん検知情報算定手段と、前記第3の改ざん検知情報算定手段により算定された第3の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加手段と、前記エントリ追加手段によりエントリが追加されたデータリストに係る第4の改ざん検知情報を前記暗号鍵を用いて算定する第4の改ざん検知情報算定手段と、前記第4の改ざん検知情報算定手段により算定された第4の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納手段と、を備えたことを特徴とする。

【0022】この請求項6の発明によれば、外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、記憶部から第4の改ざん検知情報およびデータリストを読み出し、読み出した第4の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第1の改ざん検知情報をそれぞれ算定し、算定された第2の改ざん検知情報を含む属性情報に係る第3の改ざん検知情報を暗号鍵を用いて算定し、算定された第3の改ざん検知情報を含むデータエントリを作成し、記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第4の改ざん検知情報を算定し、算定された第4の改ざん検知情報と複数のコンテンツとを記憶部に格納することとしたので、電子データが複数のコンテンツファイルからなる場合であっても、バージョンアップを効率良くおこなうことができる。

【0023】また、請求項7の発明に係る原本性保証電子保存装置は、前記アクセス制御手段は、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、前記第4の改ざん検知情報およびデータリストを読み出す読み出し手段と、前記読み出し手段により読み出された第4の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第1の改ざん検知手段と、前記データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第2の改ざん検知手段と、前記属性情報から複製対象となる版に係る第2の改ざん検知情報を取り出し、該第2の改ざん検知情報および前記復号鍵を用いて版管理情報の改ざん検知をおこなう第3の改ざん検知手段と、前記版管

理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該第1の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第4の改ざん検知手段と、前記記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製する複製手段と、前記複製手段により複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更する属性変更手段と、前記属性変更手段により変更された属性コードを含む属性情報および前記暗号鍵を用いて第3の改ざん検知情報を再算定する第3の改ざん検知情報再算定手段と、前記第3の改ざん検知情報再算定手段により算定された第3の改ざん検知情報を含むエントリにより前記データリストを更新し、更新後のデータリストに係る第4の改ざん検知情報を前記暗号鍵を用いて再算定する第4の改ざん検知情報再算定手段と、を備えたことを特徴とする。

【0024】この請求項7の発明によれば、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、第4の改ざん検知情報およびデータリストを読み出し、読み出した第4の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、属性情報から複製対象となる版に係る第2の改ざん検知情報を取り出し、該第2の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該第1の改ざん検知情報および復号鍵を用いて前記コンテンツファイルの改ざん検知をおこない、記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製し、複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更し、変更された属性コードを含む属性情報および暗号鍵を用いて第3の改ざん検知情報を再算定し、再算定された第3の改ざん検知情報を含むエントリによりデータリストを更新し、更新後のデータリストに係る第4の改ざん検知情報を暗号鍵を用いて再算定することとしたので、電子データが複数のコンテンツファイルからなる場合であっても、版を指定した複製を効率良くおこなうことができる。

【0025】また、請求項8の発明に係る原本性保証電子保存方法は、所定の記憶部に記憶した電子データの原本性を保証する原本性保証電子保存方法において、複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存する保存工程と、前記保存工程によって保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベ

ルのアクセス制御をおこなうアクセス制御工程と、を含んだことを特徴とする。

【0026】この請求項8の発明によれば、複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存し、保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうこととしたので、複数のファイルから形成される複合文書の原本性を効率良く保証することができる。

【0027】また、請求項9の発明に係る原本性保証電子保存方法は、前記保存工程は、前記電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに前記記憶部に保存することを特徴とする。

【0028】この請求項9の発明によれば、電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに記憶部に保存することとしたので、効率良く改ざん検知をおこなうことができる。

【0029】また、請求項10の発明に係る原本性保証電子保存方法は、前記保存工程は、前記電子データに対応する第1の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第2の改ざん検知情報を算定し、算定した第2の改ざん検知情報を前記属性情報とともに前記記憶部に保存することを特徴とする。

【0030】この請求項10の発明によれば、電子データに対応する第1の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第2の改ざん検知情報を算定し、算定した第2の改ざん検知情報を属性情報とともに記憶部に保存することとしたので、電子データ並びにアクセス履歴を含む改ざんを効率良く検知することができる。

【0031】また、請求項11の発明に係る原本性保証電子保存方法は、前記保存工程は、前記複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第1の改ざん検知情報をそれぞれ算定する第1の改ざん検知情報算定工程と、前記第1の改ざん検知情報算定工程により算定された第1の改ざん検知情報を含む版管理情報を作成する版管理情報作成工程と、前記版管理情報作成工程により作成された版管理情報に係る第2の改ざん検知情報を前記暗号鍵を用いて算定する第2の改ざん検知情報算定工程と、前記第2の改ざん検知情報算定工程により算定された第2の改ざん検知情報を含む属性情報に係る第3の改ざん検知情報を前記暗号鍵を用いて算定する第3の改ざん検知情報算定工程により算定された第3の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加

工程と、前記エントリ追加工程によりエントリが追加されたデータリストに係る第4の改ざん検知情報を前記暗号鍵を用いて算定する第4の改ざん検知情報算定工程と、前記第4の改ざん検知情報算定工程により算定された第4の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納工程と、を含んだことを特徴とする。

【0032】この請求項11の発明によれば、複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第1の改ざん検知情報をそれぞれ算定し、算定した第1の改ざん検知情報を含む版管理情報を作成して第2の改ざん検知情報を算定し、算定した第2の改ざん検知情報を含む属性情報に係る第3の改ざん検知情報を算定し、算定した第3の改ざん検知情報を含むデータエントリを作成して記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第4の改ざん検知情報を算定し、算定した第4の改ざん検知情報と複数のコンテンツとを記憶部に格納することとしたので、複数のコンテンツファイルからなる新規データを改ざん防止措置を施しつつ効率良く格納することができる。

【0033】また、請求項12の発明に係る原本性保証電子保存方法は、前記アクセス制御工程は、外部から原本となるコンテンツファイルの読み出し要求を受け付けた際に、前記記憶部から第4の改ざん検知情報および前記データリストを読み出す読み出し工程と、前記読み出し工程により読み出された第4の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第1の改ざん検知工程と、前記データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、取り出したエントリに含まれる第3の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第2の改ざん検知工程と、前記記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第2の改ざん検知情報および前記復号鍵を用いて前記版管理情報の改ざん検知をおこなう第3の改ざん検知工程と、前記版管理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該第1の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第4の改ざん検知工程と、前記コンテンツファイルが改ざんされていない場合に、前記記憶部に記憶したコンテンツファイルを要求元に提供する提供工程と、を含んだことを特徴とする。

【0034】この請求項12の発明によれば、外部から原本となるコンテンツファイルの読み出し要求を受け付けた際に、記憶部から第4の改ざん検知情報およびデー

タリストを読み出し、読み出した第4の改ざん検知情報および復号鍵を用いてデータリストの改ざん検知をおこない、データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、このエントリに含まれる第3の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第2の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該第1の改ざん検知情報および復号鍵を用いてコンテンツファイルの改ざん検知をおこない、コンテンツファイルが改ざんされていない場合に、記憶部に記憶したコンテンツファイルを要求元に提供することとしたので、多段階に渡って改ざんを防止しつつコンテンツファイルの読み出しを効率良くおこなうことができる。

【0035】また、請求項13の発明に係る原本性保証電子保存方法は、前記アクセス制御工程は、外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、前記記憶部から第4の改ざん検知情報およびデータリストを読み出す読み出し工程と、前記読み出し工程により読み出された第4の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第1の改ざん検知工程と、前記データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第2の改ざん検知工程と、前記暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第1の改ざん検知情報をそれぞれ算定する第1の改ざん検知情報算定工程と、前記第2の改ざん検知情報算定工程により算定された第2の改ざん検知情報を含む属性情報に係る第3の改ざん検知情報を前記暗号鍵を用いて算定する第3の改ざん検知情報算定工程と、前記第3の改ざん検知情報算定工程により算定された第3の改ざん検知情報を含むデータエントリを作成し、前記記憶部に記憶したデータリストに当該データエントリを追加するエントリ追加工程と、前記エントリ追加工程によりエントリが追加されたデータリストに係る第4の改ざん検知情報を前記暗号鍵を用いて算定する第4の改ざん検知情報算定工程と、前記第4の改ざん検知情報算定工程により算定された第4の改ざん検知情報と前記複数のコンテンツとを前記記憶部に格納するデータ格納工程と、を含んだことを特徴とする。

【0036】この請求項13の発明によれば、外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、記憶部から第4の改ざん検知情報およびデータリス

トを読み出し、読み出した第4の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第1の改ざん検知情報をそれぞれ算定し、算定された第2の改ざん検知情報を含む属性情報に係る第3の改ざん検知情報を暗号鍵を用いて算定し、算定された第3の改ざん検知情報を含むデータエントリを作成し、記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第4の改ざん検知情報を算定し、算定された第4の改ざん検知情報と複数のコンテンツとを記憶部に格納することとしたので、電子データが複数のコンテンツファイルからなる場合であっても、バージョンアップを効率良くおこなうことができる。

【0037】また、請求項14の発明に係る原本性保証電子保存方法は、前記アクセス制御工程は、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、前記第4の改ざん検知情報およびデータリストを読み出す読み出し工程と、前記読み出し工程により読み出された第4の改ざん検知情報および前記暗号鍵に対応する復号鍵を用いて、前記データリストの改ざん検知をおこなう第1の改ざん検知工程と、前記データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および前記復号鍵を用いて前記属性情報の改ざん検知をおこなう第2の改ざん検知工程と、前記属性情報から複製対象となる版に係る第2の改ざん検知情報を取り出し、該第2の改ざん検知情報および前記復号鍵を用いて版管理情報の改ざん検知をおこなう第3の改ざん検知工程と、前記版管理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該第1の改ざん検知情報および前記復号鍵を用いて前記コンテンツファイルの改ざん検知をおこなう第4の改ざん検知工程と、前記記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製する複製工程と、前記複製工程により複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更する属性変更工程と、前記属性変更工程により変更された属性コードを含む属性情報および前記暗号鍵を用いて第3の改ざん検知情報を再算定する第3の改ざん検知情報再算定工程と、前記第3の改ざん検知情報再算定工程により算定された第3の改ざん検知情報を含むエントリにより前記データリストを更新し、更新後のデータリストに係る第4の改ざん検知情報を前記暗号鍵を用いて再算定する第4の改ざん検知情報再算定工程と、を含んだことを特徴とする。

【0038】この請求項14の発明によれば、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、第4の改ざん検知情報およびデータリストを読み出し、読み出した第4の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、属性情報から複製対象となる版に係る第2の改ざん検知情報を取り出し、該第2の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該第1の改ざん検知情報および復号鍵を用いて前記コンテンツファイルの改ざん検知をおこない、記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製し、複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更し、変更された属性コードを含む属性情報および暗号鍵を用いて第3の改ざん検知情報を再算定し、再算定された第3の改ざん検知情報を含むエントリによりデータリストを更新し、更新後のデータリストに係る第4の改ざん検知情報を暗号鍵を用いて再算定することとしたので、電子データが複数のコンテンツファイルからなる場合であっても、版を指定した複製を効率良くおこなうことができる。

【0039】また、請求項15の発明に係る記録媒体は、前記請求項8～14のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項8～14の動作をコンピュータによって実現することができる。

【0040】

【発明の実施の形態】以下に添付図面を参照して、この発明に係る原本性保証電子保存方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【0041】図1は、本実施の形態で用いる原本性保証電子保存装置の構成を示すブロック図である。同図に示すように、この原本性保証電子保存装置100は、原本となる電子データを記憶し、ネットワークを介してホスト計算機110からアクセスされる装置であり、大容量記憶媒体101と、通信ポート102と、プログラム格納媒体103と、内部記憶媒体104と、タイマ105と、プロセッサ106とからなる。

【0042】大容量記憶媒体101は、原本となる電子データなどを記憶する大容量の二次記憶装置であり、たとえば光磁気ディスクやCD-Rなどからなる。通信ポート102は、ネットワークを介したホスト計算機との

通信をおこなうためのインターフェース部であり、たとえばLANカードなどの通信モデムなどからなる。

【0043】プログラム格納媒体103は、主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを格納したメモリであり、たとえば書換可能なEEPROMや読み出し専用のROMなどからなる。

【0044】内部記憶媒体104は、各種プログラムの実行に必要なパラメータを記憶するEEPROMなどからなるメモリであり、具体的には、装置暗号鍵、装置復号鍵、媒体認証コードリスト、最新データ識別番号、タイマ設定履歴ファイルおよびアカウント管理リストなどを記憶する。タイマ105は、プロセッサ106がプログラムの実行時に所得する時刻を計時するタイマである。

【0045】なお、大容量記憶媒体101については、図中に破線で示したように原本性保証電子保存装置100から取り外し可能としても良いが、その他の構成部位については原本性保証電子保存装置100と物理的に一体化し、通信ポート102以外からのアクセスを受け付けない耐タンパー性を有する構成にする。

【0046】ただし、この耐タンパー性には、筐体を開けられないようにシールを貼る程度のレベルから、筐体を開けた場合に装置が動作しなくなるレベルまで様々なものがあるが、本発明はこの耐タンパー性のレベルには特段の制限を受けない。

【0047】プロセッサ106は、プログラム格納媒体103に格納された主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを読み出して実行する制御装置である。

【0048】具体的には、このプロセッサ106は、ユーザから保存要求のあったデータを大容量記憶媒体101に保存する際に、あとでデータの改ざんを検出できるようにするために、内部記憶媒体104に記憶したプライベートキーを用いて保存するデータにメッセージ認証子(MAC: Message Authentication Code)を付加する。なお、このメッセージ認証子は、たとえば公開鍵暗号方式を採用した場合には、ディジタル署名として付加するデータに該当する。

【0049】また、データそのものの不正な抹消を検出するために、大容量記憶媒体101に記憶されているデータのリストに対してもメッセージ認証子を付加し、さらにたとえば大容量記憶媒体101の状態を過去の状態に戻すような不正なすり替えを検出するために、大容量記憶媒体101の媒体識別番号と、その媒体のデータリストに対するメッセージ認証子の対を内部記憶媒体104に記憶して管理する。

【0050】また、データ作成日などを不正に変更することができないように、タイマ105から現在時刻を取

19

得し、この時刻をデータの属性として付与するとともに、原本性保証電子保存装置100内部でオリジナルな電子データである原本データとそのコピーとを区別することができるように、「仮原本」、「原本」および「謄本」といった属性をデータに付与して管理する。たとえば、「原本」という属性が付与されたデータをコピーした場合には、このコピーしたデータに「謄本」という属性が付与される。

【0051】なお、この属性は外部から変更することはできず、また大容量記憶媒体101を取り外して外部にてその属性を改ざんしたとしても、この大容量記憶媒体101を装置に装着した際に改ざんの有無を検出する。

【0052】次に、図1に示した大容量記憶媒体101に保存する保存データのデータ構造について説明する。図2は、図1に示した大容量記憶媒体101に保存する保存データのデータ構造の一例を示す説明図である。同図に示すように、この保存データ200は、バージョン1に係るデータ210と、バージョン2に係るデータ220と、バージョン3に係るデータ230とからなる。

【0053】そして、このバージョン1の段階では、コンテンツ1～3という3つのコンテンツを有しているが、バージョン2になる際にコンテンツ4が付加され、さらにバージョン3になる際に3番目のコンテンツ3が削除されている。

【0054】このように、かかる大容量記憶媒体101に保存する保存データは、複数のコンテンツからなるデータ

具体的には、

/documents

/R01093-00123210

R01093-00123210.dat

/ver.1

R01093-00123210-1.dat

index.htm

icon.gif

context.htm

/ver.2

R01093-00123210-2.dat

context.htm

/R01093-00123211

R01093-00123211.dat

/ver.1

R01093-00123211-1.dat

main.xml

theme.dtd

theme.xsl

/C-R03055-00000107

C-R03055-00000107.dat

/ver.5

C-R03055-00000107-5.dat

frontpaper.doc

20

ータを各バージョンごとに保存している。なお、図中に破線で示すコンテンツは、コンテンツ属性情報のみが存在するものであり、コンテンツデータファイルそのものは前バージョンのコンテンツデータファイルを参照するよう構成している。

【0055】次に、図1に示した大容量記憶媒体101に保存する保存データの配置について説明する。保存データは、データ識別番号（たとえば「R01093-00123210」）をフォルダ名とするフォルダの下に、該データ識別番号をファイル名とするデータ属性情報ファイル（たとえば「R01093-00123210.dat」）を格納し、バージョンごとにバージョン番号をフォルダ名とするフォルダ（たとえば「ver.1」）を作成して、そのフォルダ内にコンテンツのデータファイルとバージョン属性情報ファイルとを格納する。

【0056】バージョン属性情報ファイルは、ファイル名としてデータ識別番号の後ろにバージョン番号をつけたもの（たとえば「R01093-00123210-1.dat」）とし、謄本データについては、謄本データであることが直ちに判明するようにデータ識別番号の先頭に「C-」を含める。

【0057】また、原本性保証電子保存装置100が独自に管理するファイル、たとえば媒体識別番号ファイルおよび保存データリストファイルは、保存データとは別のフォルダ（system）に格納する。

【0058】

; データごとのフォルダ

; データ属性情報ファイル

; バージョンごとのフォルダ

; バージョン属性情報ファイル

; コンテンツデータ # 1

; コンテンツデータ # 2

; コンテンツデータ # 3

toc.doc
chapter1.doc
chapter2.doc
appendix.doc

/...

/system

medium.id

R01093-0012.list

のように保存データの配置を記述する。

【0059】次に、図1に示した原本性保証電子保存装置100による新規データの保存処理について図3～図8を用いて説明する。図3は、図1に示した原本性保証電子保存装置100による新規データの保存処理手順を示すフローチャートである。

【0060】図3に示すように、原本性保証電子保存装置100は、まず最初に大容量記憶媒体101がマウントされているか否かを判定し（ステップS301）、大容量記憶媒体101がマウントされていない場合には（ステップS301肯定）、エラー処理をおこなった後に（ステップS302）、処理を終了する。

【0061】これに対して、大容量記憶媒体101がマウントされている場合には（ステップS301否定）、通信ポート102を介して外部からデータ属性コード、コンテンツ数、コンテンツ名およびコンテンツデータを受け取る（ステップS303）。そして、受け取ったデータ属性コードが「原本」、「仮原本」または「一般」のいずれかでか該当するか否かを確認し（ステップS304）、いずれにも該当しない場合には（ステップS305肯定）、エラー処理をおこなった後に（ステップS302）、処理を終了する。

【0062】これに対して、このデータ属性コードが「原本」、「仮原本」または「一般」のいずれかであれば（ステップS304否定）、データ属性コードが「一般」であるか否かをさらに判断し（ステップS305）、「一般」である場合には（ステップS305肯定）、受け取ったデータを受け取ったデータ名で大容量記憶媒体101に保存して処理を終了する（ステップS306）。

【0063】一方、このデータ属性コードが「一般」でない場合には（ステップS305否定）、初版としてバージョン属性情報の作成処理をおこなった後に（ステップS307）、データ属性情報を作成処理する（ステップS308）。

【0064】その後、受け取ったコンテンツデータをすべてデータファイルとして大容量記憶媒体101に保存し（ステップS309）、バージョン属性情報をバージョン属性情報ファイルとして大容量記憶媒体101に保存し（ステップS310）、データ属性情報をデータ属性情報ファイルとして大容量記憶媒体101に保存した後に（ステップS311）、保存データリストエントリ

；媒体識別番号ファイル

；保存データリストファイル

を追加して（ステップS312）、処理を終了する。

【0065】次に、図3のステップS307に示したバージョン属性情報の作成処理についてさらに具体的に説明する。図4は、図3のステップS307に示したバージョン属性情報の作成処理手順を示すフローチャートである。同図に示すように、まず最初に、内部タイマ105から現在時刻を取得し（ステップS401）、内部記憶媒体104から最新タイムIDを取得する（ステップS402）。

【0066】その後、対象コンテンツすべてに対してコンテンツ属性情報を作成するとともに（ステップS403）、バージョン番号、現在時刻、タイムID、コンテンツ数、すべてのコンテンツ属性情報などを含むバージョン属性情報を作成する（ステップS404）。

【0067】そして、バージョン属性情報に対して改ざん検知コードの計算処理をおこない、バージョン属性MACを取得し（ステップS405）、取得したバージョン属性MACをバージョン属性情報に付与して（ステップS406）、処理を終了する。なお、この改ざん検知コードの計算処理としては、保存するデータに対してハッシュ値を計算するとともに、内部記憶媒体104から装置暗号鍵を取得し、ハッシュ値を装置暗号鍵で暗号化してメッセージ認証子とする処理をおこなう。

【0068】図5は、上記ステップS403に示したコンテンツ属性情報の作成処理手順を示すフローチャートである。同図に示すように、コンテンツ情報を作成する際には、まず最初に受け取ったデータに対して改ざん検知コードの計算処理をおこない、コンテンツ属性MACを取得する（ステップS501）。

【0069】そして、内部タイマ105から現在時刻を取得し（ステップS502）、内部記憶媒体104から最新タイムIDを取得して（ステップS503）、対象データのコンテンツ番号、現在時刻、タイムID、対象データを保存する際のファイル名、対象データのサイズおよびコンテンツ属性MACなどを含むコンテンツ属性情報を作成する（ステップS504）。

【0070】次に、図3のステップS308に示したデータ属性情報の作成処理について説明する。図6は、図3のステップS308に示したデータ属性情報の作成処理手順を示すフローチャートである。

【0071】同図に示すように、まず最初に内部記憶媒体104から最新データ識別番号を取得し（ステップS

601)、最新データ識別番号を1増加させて内部記憶媒体104に記録し(ステップS602)、対象データのバージョン属性情報からバージョン属性MACなどの簡易バージョン属性情報を取得する(ステップS603)。

【0072】そして、最新データ識別番号、データ属性コード、作成日時情報、最終更新日時情報、簡易バージョン属性情報などを含むデータ属性情報を作成した後(ステップS604)、このデータ属性情報に対して改ざん検知コードの計算処理をおこなってデータ属性MACを取得し(ステップS605)、取得したデータ属性MACをデータ属性情報に付与する(ステップS606)。

【0073】次に、図3のステップS312に示した保存データリストエントリの追加処理についてさらに詳細に説明する。図7は、図3のステップS312に示した保存データリストエントリの追加処理手順を示すフローチャートである。

【0074】同図に示すように、まず大容量記憶媒体101から保存データリストファイルを読み出し(ステップS701)、保存データリストに、データ識別番号、データ属性コードおよびデータ属性MACなどを含む新しいデータエントリを追加する(ステップS702)。

【0075】そして、保存データリストに対して改ざん検知コードの計算処理をおこなってリストMACを取得し(ステップS703)、このリストMACを保存データリストに付与し(ステップS704)、保存データリストを大容量記憶媒体101に保存した後に(ステップS705)、リストMACをもとに内部記憶媒体104の媒体認証コードリストの対象エントリを更新する(ステップS706)。

【0076】次に、図3～図7において説明した新規データの保存処理の具体例について説明する。図8は、図3～図7において説明した新規データの保存処理の一例を示す説明図である。なおここでは、データ属性コードが「原本」であり、コンテンツ名がそれぞれ「chapter1.doc」および「chapter2.doc」であるコンテンツ1およびコンテンツ2からなる新規データを保存する場合を示すこととする。

【0077】同図に示すように、原本性保証電子保存装置100に新規に保存されるコンテンツ1および2についてハッシュ値をそれぞれ計算し、計算したハッシュ値を装置暗号鍵で暗号化してコンテンツ属性MACを取得する。そして、このコンテンツ属性MACを含めたコンテンツ属性情報を作成し、作成したコンテンツ属性情報を含むバージョン属性情報を作成する。

【0078】その後、このバージョン属性情報からハッシュ値を計算し、計算したハッシュ値を装置暗号鍵で暗号化してバージョン属性MACを取得して、取得したバージョン属性MACをバージョン属性情報に追加する。

【0079】また、このバージョン属性MACを含むデータ属性情報を作成し、作成したデータ属性情報からハッシュ値を計算し、計算したハッシュ値を装置暗号鍵で暗号化してデータ属性MACを取得して、取得したデータ属性MACをデータ属性情報に付加する。

【0080】そして、コンテンツ1および2、バージョン属性情報およびデータ属性情報をそれぞれデータファイル、バージョン属性情報ファイルおよびデータ属性情報ファイルとして大容量記憶媒体101に格納するとともに、保存データリストの内容を更新する。

【0081】上記図3～図8に示した一連の処理をおこなうことにより、複数のコンテンツからなる保存データを原本性を保証しつつ大容量記憶媒体101に新規保存することができる。

【0082】次に、大容量記憶媒体101のマウント処理について説明する。図9は、図1に示した大容量記憶媒体101のマウント処理手順を示すフローチャートである。同図に示すように、まず最初に装着された大容量記憶媒体101がフォーマットされているか否かを調べ(ステップS901)、フォーマットされていない場合には(ステップS901肯定)、大容量記憶媒体101をフォーマットする(ステップS902)。

【0083】具体的には、媒体を初期化し、内部記憶媒体104から媒体認証コードリストを取得し、媒体認証コードリストから最新の媒体識別番号を取得し、媒体識別番号を1増加させた新しい媒体識別番号を大容量記憶媒体101に記録し、内部記憶媒体104の媒体認証コードリストに新しい媒体識別番号のエントリを追加する(リストMACなし)という手順で大容量媒体101をフォーマットする。

【0084】そして、装着された大容量記憶媒体がフォーマット済みの場合(ステップS901否定)またはステップS902によるフォーマット処理を終了した場合には、保存データリストファイルを改ざん検知読み出し処理する(ステップS903)。

【0085】具体的には、対象ファイルを読み出し、対象ファイルに記録されたメッセージ認証子とデータを分離し、データに対してハッシュ値を計算し、内部記憶媒体104から装置暗号鍵を取得し、装置復号鍵でメッセージ認証子を復号して検証用ハッシュ値とし、先のハッシュ値が検証用ハッシュ値と一致しない場合には改ざんされたものと判断する処理をおこなう。

【0086】そして、改ざんがなされていると判断された場合には(ステップS904肯定)、エラー処理をおこない(ステップS910)、改ざんがなされていないと判断された場合には(ステップS904否定)、大容量記憶媒体101から媒体識別番号を取得し(ステップS905)、この媒体識別番号に該当するメッセージ認証子(リストMAC)を内部記憶媒体104から取得するとともに(ステップS906)、保存データリストフ

ファイルに付与されたメッセージ認証子を取得する（ステップS907）。

【0087】そして、両メッセージ認証子が同じであるならば（ステップS908否定）、認証に成功（ステップS909）したものと正常終了し、両メッセージ認証子が異なる場合には（ステップS908肯定）、エラー処理する（ステップS910）。

【0088】上記一連の処理をおこなうことにより、大容量記憶媒体101が取り外し可能な場合に、この大容量記憶媒体101のマウント時にその正当性を検証することができる。

【0089】次に、図1に示した原本性保証電子保存装置100によるデータ読み出し処理について説明する。図10および図11は、図1に示した原本性保証電子保存装置100によるデータ読み出し処理手順を示すフローチャートである。

【0090】同図に示すように、まず最初に大容量記憶媒体101がマウントされているか否かを調べ（ステップS1001）、大容量記憶媒体101がマウントされていない場合には（ステップS1001肯定）、エラー処理をおこなって（ステップS1002）処理を終了する。

【0091】これに対して、大容量記憶媒体101がマウントされている場合には（ステップS1001否定）、大容量記憶媒体101の保存データリストファイルを読み出し（ステップS1003）、この保存データリストから対象データのエントリを取得する（ステップS1004）。

【0092】そして、対象データのエントリが存在するかどうかを調べ（ステップS1005）、該当するエントリが存在しない場合には（ステップS1005肯定）、大容量記憶媒体101から対象データファイルを読み出し（ステップS1006）、読み出しデータを外部システムに送出して（ステップS1007）、処理を終了する。

【0093】これに対して、対象データのエントリが存在する場合には（ステップS1005否定）、大容量記憶媒体101から対象データのデータ属性情報ファイルを読み出し（ステップS1009）、データ属性情報に対して改ざん検知コード検証処理をおこなう（ステップS1010）。

【0094】そして、改ざんされているか否かを確認し（ステップS1011）、改ざんされている場合には（ステップS1011肯定）、エラー処理をおこなった後に処理を終了し（ステップS1002）、改ざんされていない場合には（ステップS1011否定）、取得したデータ属性情報からデータ属性MACを取得し（ステップS1012）、取得したデータ属性MACと先のデータ属性MACとが一致するか否かを確認する（ステップS1013）。

【0095】その結果、両者が一致しない場合には（ステップS1013肯定）、エラー処理をおこなった後に処理を終了し（ステップS1002）、両者が一致する場合には（ステップS1013否定）、外部システムがバージョン番号を指定しているか否かを確認する（ステップS1014）。そして、バージョン番号が指定されていない場合には（ステップS1014肯定）、対象バージョンを最新版とする（ステップS1015）。

【0096】その後、データ属性情報から対象バージョンのバージョン属性MACを取得し（ステップS1016）、大容量記憶媒体101から対象バージョンのバージョン属性情報ファイルを読み出して（ステップS1017）、バージョン属性情報ファイルに対して改ざん検知コード検証処理をおこない（ステップS1018）、改ざんされているか否かを確認する（ステップS1019）。

【0097】その結果、改ざんされている場合には（ステップS1019肯定）、エラー処理をおこなった後に処理を終了し（ステップS1002）、改ざんされていない場合には（ステップS1019否定）、取得したバージョン属性情報からバージョン属性MACを取得し（ステップS1020）、取得したバージョンMACと先のバージョン属性MACが一致するか否かを調べる（ステップS1021）。

【0098】そして、両者が一致しない場合には（ステップS1021肯定）、エラー処理をおこなった後に処理を終了し（ステップS1002）、両者が一致する場合には（ステップS1021否定）、大容量記憶媒体101から対象データの対象バージョンの対象コンテンツのデータファイルを読み出す（ステップS1022）。

【0099】なお、対象データファイルが存在しない場合には（ステップS1023肯定）、対象バージョンの前のバージョンの対象コンテンツのデータファイルを読み出す（ステップS1024）。

【0100】その後、読み出したデータに対してハッシュ値を計算し（ステップS1025）、バージョン属性情報から対象コンテンツのコンテンツ属性MACを取得して（ステップS1026）、コンテンツ属性MACを装置復号鍵で復号してハッシュ値を取得する（ステップS1027）。

【0101】そして、取得したハッシュ値と先に計算したハッシュ値とが一致するか否かを確認し（ステップS1028）、一致しない場合には（ステップS1028肯定）、エラー処理をおこなって処理を終了する（ステップS1002）。これに対して、取得したハッシュ値と先に計算したハッシュ値とが一致する場合には（ステップS1028否定）、読み出したデータを外部システムに送出する（ステップS1029）。

【0102】上記一連の処理をおこなうことにより、外部システムからデータ読み出し要求を受け取ると、対象

データの正当性を検証した後に、該当するデータを外部システムに送出することができる。

【0103】次に、図1に示した原本性保証電子保存装置100による謄本作成処理について説明する。図12～図15は、図1に示した原本性保証電子保存装置100による謄本作成処理手順を示すフローチャートである。

【0104】この原本性保証電子保存装置100では、「原本」の属性を持つデータに対して外部から複製要求を受け取ると、対象データファイルと、それに関連づけられたデータ属性情報ファイルおよびバージョン属性情報ファイルとを複写し、新たなデータ属性ファイルには「謄本」のデータ属性コードを付加する。

【0105】また、謄本の作成先が別の原本性保証電子保存装置の場合には、作成先の原本性保証電子保存装置にログインしてファイルを転送する。なお、ログインの手順については外部システムが原本性保証電子保存装置にログインする場合と同様の手順でおこなう。さらに、原本性保証電子保存装置間でやりとりされるデータの保護についても、外部システムと原本性保証電子保存装置との間でやりとりするデータの保護方法と同じである。

【0106】また、この謄本作成処理においても、データ保存処理と同様に保存データリストの更新をおこない、データ転送先の原本性保証電子保存装置では転送受け入れ処理がおこなわれる。

【0107】バージョン番号が指定されると、対象バージョンのデータファイルのみがコピーされバージョン番号が指定されない場合には、全バージョンがコピーされ、バージョン番号として「-1」が指定されると、最新バージョンのみがコピーされる。

【0108】具体的には、図12～図15に示すように、まず最初に大容量記憶媒体101がマウントされているか否かを調べ（ステップS1101）、マウントされていない場合には（ステップS1101肯定）、エラー処理をおこなった後に（ステップS1102）処理を終了する。

【0109】これに対して、マウントされている場合には（ステップS1101否定）、大容量記憶媒体101から保存データリストファイルを読み出し（ステップS1103）、保存データリストから対象データのエントリを取得する（ステップS1104）。なお、対象データのエントリが存在しない場合には（ステップS1105肯定）、エラー処理をおこなった後に処理を終了する（ステップS1102）。

【0110】その後、エントリからデータ属性コードを取得し（ステップS1106）、データ属性コードが「原本」であるか否かを調べ（ステップS1107）、「原本」でない場合には（ステップS1107肯定）、エラー処理をおこなった後に処理を終了する（ステップS1102）。

【0111】これに対して、データ属性コードが「原本」である場合には（ステップS1107否定）、エントリからデータ属性MACを取得し（ステップS1108）、対象データのデータ属性情報ファイルを読み出し（ステップS1109）、データ属性情報に対して改ざん検知コード検証処理をおこない（ステップS1110）、改ざんされているか否かを確認する（ステップS1111）。

【0112】その結果、改ざんされている場合には（ステップS1111肯定）、エラー処理をおこなった後に処理を終了し（ステップS1102）、改ざんされていない場合には（ステップS1111否定）、データ属性情報からデータ属性MACを取得し（ステップS1112）、取得したデータ属性MACと先のデータ属性MACとが一致するか否かを確認し（ステップS1113）、両者が一致しない場合には（ステップS1113肯定）、エラー処理をおこなった後に処理を終了する（ステップS1102）。

【0113】これに対して、両者が一致する場合には（ステップS1113否定）、バージョン番号が指定されているか否かを確認し（ステップS1114）、このバージョン番号が指定されていない場合には（ステップS1114肯定）、対象バージョンを全バージョンとする（ステップS1115）。また、バージョン番号が「-1」の場合には（ステップS1116肯定）、対象バージョンを最新版とする（ステップS1117）。

【0114】その後、データ属性情報から対象バージョンのバージョン属性MACを取得し（ステップS1118）、対象バージョンのバージョン属性情報ファイルを読み出し（ステップS1119）、バージョン属性情報に対して改ざん検知コード検証処理をおこなって（ステップS1120）、改ざんされているか否かを確認する（ステップS1121）。

【0115】その結果、改ざんされている場合には（ステップS1121肯定）、エラー処理をおこなった後に処理を終了し（ステップS1102）、改ざんされていない場合には（ステップS1121否定）、バージョン属性情報からバージョン属性MACを取得する（ステップS1122）。

【0116】そして、取得したバージョン属性MACが先のバージョン属性MACと一致するか否かを確認し（ステップS1123）、両者が一致しない場合には（ステップS1123肯定）、エラー処理をおこなった後に処理を終了する（ステップS1102）。

【0117】これに対して、両者が一致する場合には（ステップS1123否定）、対象バージョンのコンテンツデータファイルを特定し（ステップS1124）、バージョン属性情報に含まれる全コンテンツのコンテンツ属性MACを取得して（ステップS1125）、大容量記憶媒体101から対象コンテンツデータファイルを

読み出す(ステップS1126)。

【0118】その後、対象コンテンツデータについてハッシュ値を計算し(ステップS1127)、内部記憶媒体104から装置復号鍵を取得して(ステップS1128)、コンテンツ属性MACを装置復号鍵で復号して検証用ハッシュ値を計算し(ステップS1129)、先のハッシュ値と検証用ハッシュ値が一致するか否かを確認する(ステップS1130)。

【0119】その結果、両者が一致しない場合には(ステップS1130肯定)、エラー処理をおこなった後に処理を終了し(ステップS1102)、両者が一致する場合には(ステップS1130否定)、作成先が同じ原本性保証電子保存装置内であるか否かを確認する(ステップS1131)。

【0120】そして、作成先が同じ原本性保証電子保存装置内である場合には(ステップS1131肯定)、内部記憶媒体104から最新データ識別番号を取得し(ステップS1132)、最新データ識別番号を1増加させて内部記憶媒体104に記録する(ステップS1133)。

【0121】その後、対象データの対象バージョンのコンテンツデータファイルを作成先にコピーし(ステップS1134)、対象データの対象バージョンのバージョン属性情報ファイルを作成先にコピーし(ステップS1135)、対象データのデータ属性情報ファイルを作成先にコピーする(ステップS1136)。

【0122】そして、作成先のデータ属性情報ファイルを読み出し処理し(ステップS1137)、データ属性情報のデータ属性コードを「謄本」に変更し(ステップS1138)、データ属性情報の参照原本識別番号に現在のデータ識別番号を設定する(ステップS1139)。

【0123】また、データ属性情報のデータ識別番号を新しいデータ識別番号に変更し(ステップS1140)、内部タイマ105から現在時刻を取得し(ステップS1141)、データ属性情報に謄本作成履歴(ユーザ名、現在時刻、タイマID等)を追加する(ステップS1142)。

【0124】そして、データ属性情報に対して改ざん検知コード計算処理をおこなってデータ属性MACを取得し(ステップS1143)、データ属性情報にデータ属性情報MACを付与し(ステップS1144)、データ属性情報を大容量記憶媒体101にデータ属性情報ファイルとして保存して(ステップS1145)、保存データリストファイルを追加処理する(ステップS1146)。

【0125】また、上記ステップS1131において、作成先が同じ原本性保証電子保存装置内でない場合には(ステップS1131否定)、作成先の原本性保証電子保存装置にログインし(ステップS1146)、対象デ

ータの対象バージョンのコンテンツデータを作成先の原本性保証電子保存装置に謄本作成モードで転送する(ステップS1147)。

【0126】また、対象データの対象バージョンのバージョン属性情報を作成先の原本性保証電子保存装置に謄本作成モードで転送し(ステップS1148)、対象データのデータ属性情報を作成先の原本性保証電子保存装置に謄本作成モードで転送して(ステップS1149)、作成先の原本性保証電子保存装置からログアウトする(ステップS1150)。

【0127】次に、図1に示した原本性保証電子保存装置100のデータ移動処理について説明する。図16および図17は、図1に示した原本性保証電子保存装置100のデータ移動処理手順を示すフローチャートである。なお、ここでは移動を全バージョン一括でしかおこなえないものとする。

【0128】同図に示すように、まず最初に大容量記憶媒体101がマウントされているか否かを判断し(ステップS1301)、マウントされていない場合には(ステップS1301肯定)、エラー処理をおこなった後に(ステップS1302)処理を終了する。

【0129】これに対して、大容量記憶媒体101がマウントされている場合には(ステップS1301否定)、大容量記憶媒体101から保存データリストファイルを読み出し(ステップS1303)、保存データリストから対象データのエントリを取得する(ステップS1304)。なお、対象データのエントリが存在しない場合には(ステップS1305肯定)、対象データのデータファイルを移動モードで転送した後に(ステップS1306)、対象データのデータファイルを大容量記憶媒体101から削除して(ステップS1307)、処理を終了する。

【0130】そして、対象データのエントリが存在する場合には(ステップS1305否定)、エントリからデータ属性MACを取得し(ステップS1308)、対象データのデータ属性情報ファイルを読み出し(ステップS1309)、データ属性情報に対して改ざん検知コード検証処理をおこない(ステップS1310)、改ざんされているか否かを確認する(ステップS1311)。

【0131】その結果、改ざんされている場合には(ステップS1311肯定)、エラー処理をおこなった後に処理を終了し(ステップS1302)、改ざんされていない場合には(ステップS1311否定)、データ属性情報からデータ属性MACを取得し(ステップS1312)、取得したデータ属性MACと先のデータ属性MACが一致するか否かを確認し(ステップS1313)、両者が一致しない場合には(ステップS1313肯定)、エラー処理をおこなった後に処理を終了する(ステップS1302)。

【0132】これに対して、両者が一致する場合には

(ステップS1313否定)、データ属性情報から全バージョンのバージョン属性MACを取得し(ステップS1314)、全バージョンのバージョン属性情報ファイルを読み出し(ステップS1315)、各バージョン属性情報に対して改ざん検知コード検証処理をおこない

(ステップS1316)、改ざんされているか否かを確認する(ステップS1317)。

【0133】その結果、改ざんされている場合には(ステップS1317肯定)、エラー処理をおこなった後に処理を終了し(ステップS1302)、改ざんされていない場合には(ステップS1317否定)、各バージョン属性情報からバージョン属性MACを取得し(ステップS1318)、取得した各バージョン属性MACが先の各バージョン属性MACと一致するか否かを確認し(ステップS1319)、両者が一致しない場合には(ステップS1319肯定)、エラー処理をおこなった後に処理を終了する(ステップS1302)。

【0134】これに対して、両者が一致する場合には(ステップS1319否定)、全バージョン属性情報に含まれる全コンテンツのコンテンツ属性MACを取得し(ステップS1320)、大容量記憶媒体101から対象となる全コンテンツデータファイルを読み出す(ステップS1321)。

【0135】その後、各コンテンツデータについてハッシュ値を計算し(ステップS1322)、内部記憶媒体104から装置復号鍵を取得して(ステップS1323)、各コンテンツ属性MACを装置復号鍵で復号化して検証ハッシュ値を計算し(ステップS1324)、先のハッシュ値と各検証ハッシュ値が一致するか否かを確認する(ステップS1325)。

【0136】その結果、両者が一致しない場合には(ステップS1325肯定)、エラー処理をおこなった後に処理を終了し(ステップS1302)、両者が一致する場合には(ステップS1325否定)、移動先の原本性保証電子保存装置にログインする(ステップS1326)。

【0137】そして、全コンテンツデータを移動先の原本性保証電子保存装置に移動モードで転送し(ステップS1327)、全バージョン属性情報を移動先の原本性保証電子保存装置に移動モードで転送し(ステップS1328)、データ属性情報を移動先の原本性保証電子保存装置に移動モードで転送する(ステップS1329)。

【0138】その後、対象データの全コンテンツデータファイルを削除し(ステップS1330)、対象データの全バージョン属性情報ファイルを削除し(ステップS1331)、対象データのデータ属性情報ファイルを削除し(ステップS1332)、移動したデータに対して保存データリストエントリの削除処理をおこなった後に(ステップS1333)、移動先の原本性保証電子保存

装置からログアウトする(ステップS1334)。

【0139】図18は、図17のステップS1333で示した保存データリストエントリの削除処理手順を示すフローチャートである。同図に示すように、保存データリストエントリを削除する際には、大容量記憶媒体101から保存データリストファイルを読み出し(ステップS1401)、保存データリストから対象エントリを削除する(ステップS1402)。

【0140】そして、新しい保存データリストに対してハッシュ値を計算し(ステップS1403)、内部記憶媒体104から装置暗号鍵を取得して(ステップS1404)、装置暗号鍵でハッシュ値を暗号化してリストMACを取得する(ステップS1405)。

【0141】その後、新しい保存データリストにリストMACを付与し(ステップS1406)、保存データリストを大容量記憶媒体101に保存データリストファイルとして保存した後に(ステップS1407)、内部記憶媒体104の媒体認証コードリストを新しいリストMACで更新する(ステップS1408)。

【0142】次に、移動先の原本性保証電子保存装置における転送受け入れ処理について説明する。図19および図20は、移動先の原本性保証電子保存装置における転送受け入れ処理手順を示すフローチャートである。

【0143】同図に示すように、まず最初に大容量記憶媒体101がマウントされているか否かを判断し(ステップS1501)、マウントされていない場合には(ステップS1501肯定)、エラー処理をおこなって処理を終了する(ステップS1502)。

【0144】これに対して、大容量記憶媒体101がマウントされている場合には(ステップS1501否定)、謄本作成モードであるか否かを確認し(ステップS1503)、謄本作成モードである場合には(ステップS1503肯定)、大容量記憶媒体101から保存データリストファイルを読み出し(ステップS1504)、受け取った全コンテンツデータに対して改ざん検知コード計算処理をおこなってコンテンツ属性MACを取得し(ステップS1505)、受け取ったバージョン属性情報の中のコンテンツ属性MACを更新する(ステップS1506)。

【0145】その後、新しいバージョン属性情報に対して改ざん検知コード計算処理をおこなってバージョン属性MACを取得し(ステップS1507)、バージョン属性情報にバージョン属性MACを付与し(ステップS1508)、受け取ったデータ属性情報の中のバージョン属性MACを更新する(ステップS1509)。

【0146】また、データ属性情報のデータ属性コードを「謄本」に変更し(ステップS1510)、データ属性情報のデータ識別番号を参照原本識別番号として設定し(ステップS1511)、内部記憶媒体104から最新データ識別番号を取得する(ステップS1512)。

【0147】そして、この最新データ識別番号に1を加えた番号で内部記憶媒体104の最新データ識別番号を更新し(ステップS1513)、データ属性情報のデータ識別番号に最新データ識別番号を設定して(ステップS1514)、データ属性情報に謄本作成履歴を追加する(ステップS1515)。

【0148】そして、新しいデータ属性情報に対して改ざん検知コード計算処理をおこなってデータ属性MACを取得し(ステップS1516)、データ属性情報にデータ属性MACを付与し(ステップS1517)、受け取った全コンテンツデータをデータファイルとして大容量記憶媒体101に保存する(ステップS1518)。

【0149】また、データ属性情報を大容量記憶媒体101にデータ属性情報ファイルとして保存し(ステップS1519)、バージョン属性情報を大容量記憶媒体101にバージョン属性情報ファイルとして保存して(ステップS1520)、対象データについて保存データリストエントリ追加処理する(ステップS1521)。

【0150】これに対して、上記ステップS1503において謄本作成モードではなく移動モードである場合には(ステップS1503否定)、データ属性情報を受け取ったか否かを確認し(ステップS1522)、受け取った場合には(ステップS1522肯定)、このデータ属性情報を大容量記憶媒体101に保存する(ステップS1523)。

【0151】そして、大容量記憶媒体101から保存データリストファイルを読み出し(ステップS1524)、受け取った全コンテンツデータに対して改ざん検知コード計算処理をおこなってコンテンツ属性MACを取得し(ステップS1525)、受け取った全バージョン属性情報の中のコンテンツ属性MACを更新する(ステップS1526)。

【0152】そして、新しい全バージョン属性情報に対して改ざん検知コード計算処理をおこなってバージョン属性MACを取得し(ステップS1527)、全バージョン属性情報に各バージョン属性MACを付与し(ステップS1528)、受け取ったデータ属性情報の中の全バージョン属性MACを更新する(ステップS1529)。

【0153】そして、内部記憶媒体104から最新データ識別番号を取得し(ステップS1530)、この最新データ識別番号に1を加えた番号で内部記憶媒体104の最新データ識別番号を更新し(ステップS1531)、データ属性情報のデータ識別番号に最新データ識別番号を設定し(ステップS1532)、データ属性情報にデータ移動履歴を追加する(ステップS1533)。

【0154】そして、新しいデータ属性情報に対して改ざん検知コード計算処理をおこなってデータ属性MACを取得し(ステップS1534)、データ属性情報にデ

ータ属性MACを付与する(ステップS1535)。

【0155】その後、受け取った全コンテンツデータをデータファイルとして大容量記憶媒体101に保存し(ステップS1536)、データ属性情報を大容量記憶媒体101にデータ属性情報ファイルとして保存し(ステップS1537)、全バージョン属性情報を大容量記憶媒体101にバージョン属性情報ファイルとして保存し(ステップS1538)、対象データについて保存データリストエントリ追加処理をおこなう(ステップS1539)。

【0156】次に、図1に示した原本性保証電子保存装置100によるデータの削除処理について説明する。図21は、図1に示した原本性保証電子保存装置100によるデータの削除処理手順を示すフローチャートである。なおここでは、「原本」のデータ属性コードを持つデータは証拠隠滅を防ぐために削除しないこととする。

【0157】同図に示すように、まず最初に大容量記憶媒体101がマウントされているか否かを判断し(ステップS1601)、マウントされていない場合には(ステップS1601否定)、エラー処理をおこなって(ステップS1602)処理を終了する。

【0158】これに対して、大容量記憶媒体101がマウントされている場合には(ステップS1601肯定)、大容量記憶媒体101から保存データリストファイルを読み出し(ステップS1603)、対象データに該当するエントリを取得する(ステップS1604)。なお、エントリが存在しない場合には(ステップS1605肯定)、対象データを削除する(ステップS1606)。

【0159】その後、エントリから対象データのデータ属性コードを取得し(ステップS1607)、このデータ属性コードが「原本」であるか否かを確認する(ステップS1608)。

【0160】そして、データ属性コードが「原本」である場合には(ステップS1608肯定)、エラー処理をおこなって処理を終了し(ステップS1602)、「原本」でない場合には(ステップS1608否定)、対象データについて保存データリストエントリを削除し(ステップS1609)、対象データの全コンテンツデータファイルを削除し(ステップS1610)、対象データの全バージョン属性情報ファイルを削除し(ステップS1611)、対象データのデータ属性ファイルを削除する(ステップS1612)。

【0161】次に、図1に示した原本性保証電子保存装置100によるデータ属性コードの変更処理について説明する。データ保存処理において、「仮原本」の属性を持つデータを保存することはできるが、この「仮原本」データは単純にデータ属性コードを「原本」に変更することが可能である。

【0162】また、「謄本」、「バックアップ仮原

本」、「バックアップ原本」および「バックアップ謄本」の属性を持つデータはそれぞれ属性コードを変更することで元のデータを復旧することができる。

【0163】かかる復旧をおこなうと、図22に示すように、「謄本」が「原本」に復旧され、「バックアップ仮原本」が「仮原本」に復旧され、「バックアップ原本」が「原本」に復旧され、「バックアップ謄本」が「謄本」に復旧される。なお、かかるデータ属性コードを変更するとこれをデータアクセス履歴として記録することとなる。

【0164】また、図23および図24は、図1に示した原本性保証電子保存装置100によるデータ属性コードの変更処理手順を示すフローチャートである。同図に示すように、まず最初に大容量記憶媒体101がマウントされているか否かを確認し（ステップS1801）、マウントされていない場合には（ステップS1801肯定）、エラー処理をおこなって（ステップS1802）処理を終了する。

【0165】これに対して、大容量記憶媒体101がマウントされている場合には（ステップS1801否定）、大容量記憶媒体101から保存データリストファイルを読み出し（ステップS1803）、保存データリストから対象データに該当するエントリを取得する（ステップS1804）。なお、該当するエントリが存在しない場合には（ステップS1805肯定）、エラー処理をおこなって（ステップS1802）処理を終了する。

【0166】その後、エントリから現データ属性コードを取得し（ステップS1806）、新データ属性コードが「仮原本」であり（ステップS1807肯定）、現データ属性コードが「バックアップ仮原本」である場合には（ステップS1808否定）、データ属性情報のデータ属性コードを「仮原本」に変更する（ステップS1809）。

【0167】なお、ステップS1808で現データ属性コードが「バックアップ仮原本」でない場合には（ステップS1808肯定）、エラー処理をおこなって処理を終了する（ステップS1802）。

【0168】また、新データ属性コードが「仮原本」でない場合には（ステップS1807否定）、この新データ属性コードが「原本」であるか否かを調べ（ステップS1810）、この新データ属性コードが「原本」である場合には（ステップS1810肯定）、現データ属性コードが「バックアップ仮原本」または「仮原本」であるか否かを調べる（ステップS1811）。

【0169】その結果、現データ属性コードが「バックアップ仮原本」または「仮原本」である場合には（ステップS1811否定）、データ属性情報のデータ属性コードを「原本」に変更する（ステップS1812）。

【0170】なお、ステップS1811で現データ属性コードが「バックアップ原本」または「仮原本」でない

場合には（ステップS1811肯定）、エラー処理をおこなって処理を終了する（ステップS1802）。

【0171】また、新データ属性コードが「原本」でない場合には（ステップS1810否定）、この新データ属性コードが「謄本」であるか否かを調べ（ステップS1813）、この新データ属性コードが「謄本」である場合には（ステップS1813肯定）、現データ属性コードが「バックアップ謄本」であら否かを調べ（ステップS1814）、「バックアップ謄本」である場合には（ステップS1814否定）、データ属性情報のデータ属性コードを「謄本」に変更する（ステップS1815）。

【0172】なお、ステップS1814で現データ属性コードが「バックアップ謄本」でない場合には（ステップS1814肯定）、エラー処理をおこなって処理を終了する（ステップS1802）。

【0173】そして、これらの変更を終えたならば、タイム105から現在時刻を取得し（ステップS1816）、データ属性情報にデータ属性コード変更履歴を追加して（ステップS1817）、新しいデータ属性情報を改ざん検知コード計算処理をおこなってデータ属性MACを取得して（ステップS1818）、データ属性情報にデータ属性MACを付与する（ステップS1819）。

【0174】その後、データ属性情報を大容量記憶媒体101にデータ属性情報ファイルとして保存し（ステップS1820）、対象データについて保存データリストエントリの更新処理をおこなって（ステップS1821）、処理を終了する。

【0175】図25は、図24のステップS1821に示した保存データリストエントリの更新処理手順を示すフローチャートである。同図に示すように、保存データリストエントリの更新処理では、大容量記憶媒体101から保存データリストファイルを読み出し（ステップS1901）、保存データリストの対象データに該当するエントリを更新する（ステップS1902）。

【0176】そして、保存データリストに対してハッシュ値を計算し（ステップS1903）、内部記憶媒体104から装置暗号鍵を取得して（ステップS1904）、ハッシュ値を装置暗号鍵で暗号化してリストMACを取得する（ステップS1905）。

【0177】そして、保存データリストにリストMACを付与し（ステップS1906）、保存データリストを大容量記憶媒体101に保存して（ステップS1907）、内部記憶媒体104の媒体認証コードリスト内の該当するリストMACを更新する（ステップS1908）。

【0178】次に、図1に示した原本性保証電子保存装置100によるデータのバージョンアップ処理について説明する。このデータバージョンアップ処理では、「原

本」および「仮原本」のデータ属性コードを持つデータに対しては編集を許可しないが、バージョンアップについては許可することとしている。このように、バージョンアップのみを許可することにより、以前のデータが失われず、電子データの編集履歴が分かるため、その証明力が高まることになる。

【0179】また、この原本性保証電子保存装置100では、「謄本」およびバックアップのデータについては、追記や編集を許可しない。その理由は、データの訂正や修正は、原本に対して施すべきものであり、コピーやバックアップに対して施すべきものではないからである。

【0180】また、バージョンを上げる際に、編集していないコンテンツデータファイルについては、前のバージョンのコンテンツデータファイルをそのまま参照することとし、あるバージョンを指定した謄本作成は、そのバージョンにコンテンツデータファイルがない場合には、前のバージョンを辿ってコンテンツデータファイルをコピーすることとする。

【0181】かかるバージョンアップ処理は、対象となるデータのデータ識別番号および対象コンテンツ番号を指定してコンテンツデータが外部から渡されるか、若しくは、そのコンテンツデータを削除する要求を渡すこととする。

【0182】図26は、図1に示した原本性保証電子保存装置100によるデータのバージョンアップ処理手順を示すフローチャートである。同図に示すように、大容量記憶媒体101がマウントされている場合には（ステップS2001否定）、大容量記憶媒体101から保存データリストファイルを読み出す（ステップS2003）。

【0183】そして、読み出した保存データリストから対象データのエントリを取得し（ステップS2004）、エントリに記録されているデータ属性コードが「原本」または「仮原本」であるか否かが判断される（ステップS2005）。なお「原本」または「仮原本」でない場合や（ステップS2005肯定）、大容量記憶媒体101がマウントされていない場合には（ステップS2001肯定）、エラー処理をおこなった後に（ステップS2002）処理を終了する。

【0184】そして、データ属性コードが「原本」または「仮原本」である場合には（ステップS2005否定）、エントリの中からデータ属性MACを取得するとともに（ステップS2006）、対象データに対応したデータ属性情報ファイルを読み出し（ステップS2007）、データ属性情報からデータ属性MACを取得し（ステップS2008）、両属性MACが一致するか否かを確認する（ステップS2009）。

【0185】そして、両属性MACが一致しない場合には（ステップS2009肯定）、エラー処理をおこな

て（ステップS2002）処理を終了し、両属性MACが一致する場合には（ステップS2009否定）、データ属性情報に対して改ざん検知コード検証処理をおこない（ステップS2010）、改ざんされているか否かを確認し（ステップS2011）、改ざんされている場合には（ステップS2011肯定）、エラー処理をおこなって（ステップS2002）処理を終了する。

【0186】これに対して、改ざんされていない場合には（ステップS2011否定）、読み出したデータ属性情報から最新バージョン番号を取得し（ステップS2012）、最新バージョン番号に1を加えて現バージョン番号とし（ステップS2013）、外部から受け取ったデータをコンテンツデータファイルとして大容量記憶媒体101に保存する（ステップS2014）。

【0187】そして、現バージョンのバージョン属性情報作成処理をおこない（ステップS2015）、バージョン属性情報をバージョン属性情報ファイルとして大容量記憶媒体101に保存し（ステップS2016）、現バージョンのバージョン属性情報ファイルをもとにデータ属性情報更新処理をおこなう（ステップS2017）。

【0188】そして、データ属性情報をデータ属性情報ファイルとして大容量記憶媒体101に保存し（ステップS2018）、保存データリストファイルの対象データに該当するエントリの内容を新しいデータ属性情報をもとに更新し（ステップS2019）、保存データリストエントリを更新処理する（ステップS2020）。

【0189】次に、図1に示した原本性保証電子保存装置100によるデータの編集処理について説明する。この原本性保証電子保存装置100では、「仮原本」および「原本」のデータについては修正履歴を残すことで証明力を高めるために、データに対する編集要求を拒否し、また「謄本」やバックアップは、本来編集すべき対象ではないので、同様に編集要求を拒否する。このため、結果的に「一般」のデータのみが編集可能となる。

【0190】図27は、図1に示した原本性保証電子保存装置100によるデータの編集処理手順を示すフローチャートである。同図に示すように、大容量記憶媒体101がマウントされている場合には（ステップS2101否定）、大容量記憶媒体101から保存データリストファイルを読み出し（ステップS2103）、保存データリストから対象データに該当するエントリを取得する（ステップS2104）。

【0191】なお、エントリが取得できない場合や（ステップS2105否定）、大容量記憶媒体101がマウントされていない場合には（ステップS2101肯定）、エラー処理をおこなって処理を終了する（ステップS2102）。

【0192】そして、エントリが取得された場合には（ステップS2105肯定）、対象データのデータファ

イルの編集をおこなって（ステップS2106）、処理を終了する。

【0193】次に、図1に示した原本性保証電子保存装置100へのクライアント（ホスト計算機110）からのログイン処理について説明する。この原本性保証電子保存装置100にデータを保存したりデータを読み出す前に、クライアントは原本性保証電子保存装置100にログインしなければならない。

【0194】このログイン処理としては、従来から知られているICカードを用いる技術を採用することもできるが、本実施の形態では、パスワードによる一般的なチャレンジレスポンス認証処理をおこなっている。

【0195】たとえば、電子申請システムなどの場合には、エンドユーザが電子申請書類を電子申請サーバに送付し、電子申請サーバが原本性保証電子保存装置にログインして電子申請書類を原本性保証電子保存装置に保存するという運用が考えられるが、かかる場合に、ログインするのは常に電子申請サーバであるため、原本性保証電子保存装置に保存されたデータの作成者や更新者がすべて電子申請サーバになるものと考えられる。

【0196】そこで、本実施の形態では、ログインそのものは電子申請サーバがおこなうが、その後の処理を誰の代理でおこなっているのかを設定できるようにしている。また、原本性保証電子保存装置に保存されるデータについて、作成者や更新者の名前として、この設定されたユーザ名を使用することとする。

【0197】なお、この原本性保証電子保存装置100は、内部記録媒体104のアカウント管理テーブルにあらかじめアカウント名とパスワードを記憶しており、外部システムがアクセスする場合には、外部システム用のアカウント名を使用し、原本の移動やコピーをするために他の原本性保証電子保存装置にログインする際には、原本性保証電子保存装置用のアカウントを使用することとする。

【0198】図28は、図1に示した原本性保証電子保存装置100へのクライアントからのログイン処理手順を示すフローチャートである。同図に示すように、クライアントがアカウント名とログイン要求を送信し（ステップS2201）、原本性保証電子保存装置100が、このアカウント名とログイン要求を受信したならば（ステップS2202）、内部記録媒体104からアカウント管理テーブルを取得する（ステップS2203）。

【0199】そして、クライアントがアカウント名とパスワードを送信すると（ステップS2204）、原本性保証電子保存装置100では、アカウント管理テーブルから該当するパスワードを取得し（ステップS2205）、該当するパスワードが存在しない場合には（ステップS2206肯定）、エラー処理をおこなって処理を終了する（ステップS2207）。

【0200】これに対して該当するパスワードが存在す

る場合には（ステップS2206否定）、乱数を生成してクライアントに送信する（ステップS2208～S2209）とともに、乱数とパスワードを合わせたものに対してハッシュ値を計算する（ステップS2210）。

【0201】一方、クライアントがこの乱数を受信したならば（ステップS2211）、乱数とパスワードを合わせたものに対してハッシュ値を計算し（ステップS2212）、計算したハッシュ値を送信する（ステップS2213）。

10 【0202】そして、原本性保証電子保存装置100が、このハッシュ値を受信したならば（ステップS2214）、両ハッシュ値を比較して両者が一致する場合には（ステップS2215肯定）、成功した終了コードを送信し（ステップS2216）、両者が一致しない場合には（ステップS2215否定）、エラー処理をおこなう（ステップS2218）。その後、クライアントがこの終了コードを受信（ステップS2217）したならば、代理ユーザ名を送信して（ステップS2219）ログイン処理を終了する。

20 【0203】そして、原本性保証電子保存装置100が、この代理ユーザ名を受信したならば（ステップS2220）、受け取った代理ユーザ名をアクセスユーザ名として内部に保持して（ステップS2221）処理を終了する。なお、ステップS2207およびS2218のエラー処理時には、エラーを示す旨の終了コードをクライアントに送信する。

30 【0204】次に、図1に示した原本性保証電子保存装置100による日時の管理について説明する。この原本性保証電子保存装置100では、データアクセス履歴などに記録する日時は装置内部のタイマ105から取得するが、このタイマ105は設定変更が可能であるため、タイマ105を不正に変更することによりデータアクセス日時を偽ることが可能となる。

【0205】このため、本実施の形態では、タイマ105の設定をおこなうと図29（a）に示すように、タイマ設定履歴を自動的に内部記憶媒体104に記憶するよう構成している。

40 【0206】ここで、タイマIDは、装置内部で自動的に付与されるシーケンシャルな番号であり、タイマの設定を変更する都度番号が増える。また、データアクセス履歴に含まれる日時情報にはタイマIDも含まれる。

【0207】同図に示す場合に、タイマID=3において不正に日付を1月ずらし、その後タイマID=4で日付を戻していることが分かるため、データアクセス履歴の日時にタイマID=3の履歴が付されているデータは、不正に日時を偽ろうとした可能性があることが判明する。なお、タイマ設定履歴は原本性保証電子保存装置100の内部記憶媒体104に記録する。

50 【0208】また、原本性保証電子保存装置100から他の原本性保証電子保存装置へデータを移動したりコピ

一する場合にも、データアクセス履歴の日時に不都合が生じないようにするために、図 29 (b) に示すデータアクセス履歴をデータ属性情報に取り込む。なお、このデータアクセス履歴は、データ属性情報ファイルに記憶する。

【0209】具体的には、同図に示す例では、移動先の原本性保証電子保存装置 R010-0001055 の日時 19990217 10:13:43 ID=2 が、移動元の原本性保証電子保存装置 R010-0001032 の日時 19990217 10:10:21 ID=3 に相当することが分かるため、移動したデータに不正が見つかった場合には、原本性保証電子保存装置をまたいで履歴を辿ることができる。

【0210】次に、図 1 に示した原本性保証電子保存装置 100 が用いる保存データリストファイル、データ属性情報ファイル、バージョン属性情報、コンテンツ属性情報、媒体認証コードリスト、アカウント管理リスト、日時情報およびタイマ設定履歴ファイルの一例について図 30～図 32 を用いて説明する。

【0211】図 30 (a) は、原本性保証電子保存装置 100 が用いる保存データリストファイルの一例を示す図であり、同図に示すように、この保存データリストファイルは、メッセージ認証子 (リスト MAC) と各リストエントリからなる。なお、ここで言う原本化とは、属性コードを「仮原本」から「原本」に変更することを意味する。そして、最初のリスト MAC を除いた部分が改ざん検知読み出し処理した際の保存データリストとなる。

【0212】なお、媒体識別番号は、原本性保証電子保存装置の識別番号 (たとえば、R01093) に媒体をフォーマットした順に振るシーケンシャルな番号 (たとえば、0012) をつけたもの (たとえば、R01093-0012) とする。

【0213】媒体識別番号ファイルは、媒体識別番号を内容として含む規定のファイル名 (たとえば、medium.id) のファイルとして保存する。また、保存データリストファイルは、媒体識別番号 (たとえば、R01093-0012) の後ろに、.list を付加したファイル名 (たとえば、R01093-0012.list) で保存する。

【0214】図 30 (b) は、原本性保証電子保存装置 100 が用いるデータ属性情報ファイルの一例を示す図であり、同図に示すように、このデータ属性情報ファイルは、メッセージ認証子 (リスト MAC)、属性管理データ、簡易バージョン属性情報およびアクセス履歴からなる。

【0215】そして、最初のデータ属性 MAC を除いた部分が改ざん検知読み出し処理した際のデータ属性情報となる。また、データ識別番号は、原本性保証電子保存装置識別番号 (たとえば、R01093) と、最新データ識別番号から得られる番号 (たとえば、00123210) とをつなげたもの (R01093-00123210) となる。

【0216】また、データ識別情報ファイルは、そのデータ識別番号に、.dat をつけたファイル名 (たとえば、R01093-00123210.dat) で保存する。また、謄本データの場合には、複製した元の原本データのデータ識別番号を参照原本識別番号として記録する。謄本データは、データ識別番号の前に C- を付け、C-R01093-00123210 のようにする。

【0217】図 31 (a) は、原本性保証電子保存装置 100 が用いるバージョン属性情報の一例を示す図であり、同図に示すように、このバージョン属性情報は、メッセージ認証子 (リスト MAC) と、バージョン管理データとからなる。

【0218】バージョン属性情報ファイルは、そのバージョン番号に応じてデータ識別番号にバージョン番号を付けたものに、.dat をつけたファイル名 (たとえば、ver.7 なら R01093-00123210-7.dat) で保存する。最初のバージョン属性 MAC を除いた部分が改ざん検知読み出し処理した際のバージョン属性情報となる。

【0219】図 31 (b) は、原本性保証電子保存装置 100 が用いるコンテンツ属性情報の一例を示す図であり、同図に示すように、このコンテンツ属性情報は、メッセージ認証子 (コンテンツ属性 MAC) とコンテンツ管理データからなる。

【0220】前のバージョンから更新されていないコンテンツは、前バージョンのコンテンツのデータファイルを兼用するため、現バージョンにおけるデータファイルが存在しないが、存在するものとしてコンテンツ管理データ内のデータファイル名を記録する。

【0221】図 31 (c) は、原本性保証電子保存装置 100 が用いる媒体認証リストコードの一例を示す図であり、同図に示すように、この媒体認証リストコードは、媒体識別番号およびメッセージ認証子 (リスト MAC) からなる複数の認証コードエントリにより形成される。

【0222】図 32 (a) は、原本性保証電子保存装置 100 が用いるアカウント管理リストの一例を示す図であり、同図に示すように、このアカウント管理リストは、アカウント名およびパスワードからなる各アカウントエントリからなる。なお、このアカウント管理リストは、任意の数のアカウントが登録できるような構造としているが、最初から存在するクライアント用のアカウントや、原本性保証電子保存装置用のアカウントについては図示省略している。

【0223】図 32 (b) は、原本性保証電子保存装置 100 が用いる日時情報の内容を示す図であり、同図に示すように、この日時情報は、「年」、「月」、「日」、「時」、「分」、「秒」、「GST (世界標準時) からのずれ」および「タイマ ID」からなる。

【0224】図 32 (c) は、原本性保証電子保存装置 100 が用いるタイマ設定履歴ファイルの内容を示す図

であり、同図に示すように、このタイマ設定履歴ファイルは、設定前の日時情報、設定後の日時情報およびアカウント名からなる各タイマ設定履歴からなる。

【0225】

【発明の効果】以上説明したように、請求項1の発明によれば、複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存し、保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうよう構成したので、複数のファイルから形成される複合文書の原本性を効率良く保証することができる原本性保証電子保存装置が得られるという効果を奏する。

【0226】また、請求項2の発明によれば、電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに記憶部に保存するよう構成したので、効率良く改ざん検知をおこなうことができる原本性保証電子保存装置が得られるという効果を奏する。

【0227】また、請求項3の発明によれば、電子データに対応する第1の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第2の改ざん検知情報を算定し、算定した第2の改ざん検知情報を属性情報とともに記憶部に保存するよう構成したので、電子データ並びにアクセス履歴を含む改ざんを効率良く検知することができる原本性保証電子保存装置が得られるという効果を奏する。

【0228】また、請求項4の発明によれば、複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第1の改ざん検知情報をそれぞれ算定し、算定した第1の改ざん検知情報を含む版管理情報を作成して第2の改ざん検知情報を算定し、算定した第2の改ざん検知情報を含む属性情報に係る第3の改ざん検知情報を算定し、算定した第3の改ざん検知情報を含むデータエントリを作成して記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第4の改ざん検知情報を算定し、算定した第4の改ざん検知情報と複数のコンテンツとを記憶部に格納するよう構成したので、複数のコンテンツファイルからなる新規データを改ざん防止措置を施しつつ効率良く格納することができる原本性保証電子保存装置が得られるという効果を奏する。

【0229】また、請求項5の発明によれば、外部から原本となるコンテンツファイルの読み出し要求を受け付けた際に、記憶部から第4の改ざん検知情報およびデータリストを読み出し、読み出した第4の改ざん検知情報および復号鍵を用いてデータリストの改ざん検知をおこない、データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、このエントリ

に含まれる第3の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第2の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該第1の改ざん検知情報および復号鍵を用いてコンテンツファイルの改ざん検知をおこない、コンテンツファイルが改ざんされていない場合に、記憶部に記憶したコンテンツファイルを要求元に提供するよう構成したので、多段階に渡って改ざんを防止しつつコンテンツファイルの読み出しを効率良くおこなうことができる原本性保証電子保存装置が得られるという効果を奏する。

【0230】また、請求項6の発明によれば、外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、記憶部から第4の改ざん検知情報およびデータリストを読み出し、読み出した第4の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第1の改ざん検知情報をそれぞれ算定し、算定された第2の改ざん検知情報を含む属性情報に係る第3の改ざん検知情報を暗号鍵を用いて算定し、算定された第3の改ざん検知情報を含むデータエントリを作成し、記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第4の改ざん検知情報を算定し、算定された第4の改ざん検知情報と複数のコンテンツとを記憶部に格納するよう構成したので、電子データが複数のコンテンツファイルからなる場合であっても、バージョンアップを効率良くおこなうことができる原本性保証電子保存装置が得られるという効果を奏する。

【0231】また、請求項7の発明によれば、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、第4の改ざん検知情報およびデータリストを読み出し、読み出した第4の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、属性情報から複製対象となる版に係る第2の改ざん検知情報を取り出し、該第2の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該

第1の改ざん検知情報および復号鍵を用いて前記コンテンツファイルの改ざん検知をおこない、記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製し、複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更し、変更された属性コードを含む属性情報および暗号鍵を用いて第3の改ざん検知情報を再算定し、再算定された第3の改ざん検知情報を含むエントリによりデータリストを更新し、更新後のデータリストに係る第4の改ざん検知情報を暗号鍵を用いて再算定するよう構成したので、電子データが複数のコンテンツファイルからなる場合であっても、版を指定した複製を効率良くおこなうことができる原本性保証電子保存装置が得られるという効果を奏する。

【0232】また、請求項8の発明によれば、複数のコンテンツファイルにより形成される電子データの内容を一つの原本として識別可能な状態で保存し、保存した原本の電子データと該原本の電子データ以外の電子データとで異なるレベルのアクセス制御をおこなうよう構成したので、複数のファイルから形成される複合文書の原本性を効率良く保証することができる原本性保証電子保存方法が得られるという効果を奏する。

【0233】また、請求項9の発明によれば、電子データに対応する改ざん検知情報を該電子データの属性情報として当該電子データとともに記憶部に保存するよう構成したので、効率良く改ざん検知をおこなうことができる原本性保証電子保存方法が得られるという効果を奏する。

【0234】また、請求項10の発明によれば、電子データに対応する第1の改ざん検知情報および該電子データのアクセス履歴を含む該電子データの属性情報に対応する第2の改ざん検知情報を算定し、算定した第2の改ざん検知情報を属性情報とともに記憶部に保存するよう構成したので、電子データ並びにアクセス履歴を含む改ざんを効率良く検知することができる原本性保証電子保存方法が得られるという効果を奏する。

【0235】また、請求項11の発明によれば、複数のコンテンツファイルにより形成される電子データを一つの原本として新規に保存する旨の要求を受け付けた際に、所定の暗号鍵を用いて各コンテンツファイルに係る第1の改ざん検知情報をそれぞれ算定し、算定した第1の改ざん検知情報を含む版管理情報を作成して第2の改ざん検知情報を算定し、算定した第2の改ざん検知情報を含む属性情報に係る第3の改ざん検知情報を算定し、算定した第3の改ざん検知情報を含むデータエントリを作成して記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第4の改ざん検知情報を算定し、算定した第4の改ざん検知情報と複数のコンテンツとを記憶部に格納するよう構成したので、複数のコンテンツファイルからなる

新規データを改ざん防止措置を施しつつ効率良く格納することができる原本性保証電子保存方法が得られるという効果を奏する。

【0236】また、請求項12の発明によれば、外部から原本となるコンテンツファイルの読み出し要求を受け付けた際に、記憶部から第4の改ざん検知情報およびデータリストを読み出し、読み出した第4の改ざん検知情報および復号鍵を用いてデータリストの改ざん検知をおこない、データリストから読み出し対象となるコンテンツファイルに対応するエントリを取り出し、このエントリに含まれる第3の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、記憶部から読み出し対象となるコンテンツファイルに対応する版管理情報を取り出し、該版管理情報に係る第2の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該第1の改ざん検知情報および復号鍵を用いてコンテンツファイルの改ざん検知をおこない、コンテンツファイルが改ざんされていない場合に、記憶部に記憶したコンテンツファイルを要求元に提供するよう構成したので、多段階に渡って改ざんを防止しつつコンテンツファイルの読み出しを効率良くおこなうことができる原本性保証電子保存方法が得られるという効果を奏する。

【0237】また、請求項13の発明によれば、外部から原本である電子データの版をバージョンアップする旨の要求とともに複数のコンテンツファイルを受け付けた際に、記憶部から第4の改ざん検知情報およびデータリストを読み出し、読み出した第4の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから版をバージョンアップする電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、暗号鍵を用いて外部から受け取った複数のコンテンツファイルに係る第1の改ざん検知情報をそれぞれ算定し、算定された第2の改ざん検知情報を含む属性情報に係る第3の改ざん検知情報を暗号鍵を用いて算定し、算定された第3の改ざん検知情報を含むデータエントリを作成し、記憶部に記憶したデータリストに当該データエントリを追加し、エントリが追加されたデータリストに係る第4の改ざん検知情報を算定し、算定された第4の改ざん検知情報と複数のコンテンツとを記憶部に格納するよう構成したので、電子データが複数のコンテンツファイルからなる場合であっても、バージョンアップを効率良くおこなうことができる原本性保証電子保存方法が得られるという効果を奏する。

【0238】また、請求項14の発明によれば、外部から原本となる電子データの版を指定した複製要求を受け付けた際に、第4の改ざん検知情報およびデータリスト

を読み出し、読み出した第4の改ざん検知情報および暗号鍵に対応する復号鍵を用いて、データリストの改ざん検知をおこない、データリストから複製対象となる電子データのエントリを取り出し、該エントリに含まれる第3の改ざん検知情報および復号鍵を用いて属性情報の改ざん検知をおこない、属性情報から複製対象となる版に係る第2の改ざん検知情報を取り出し、該第2の改ざん検知情報および復号鍵を用いて版管理情報の改ざん検知をおこない、版管理情報から読み出し対象となるコンテンツファイルに係る第1の改ざん検知情報を取り出し、該第1の改ざん検知情報および復号鍵を用いて前記コンテンツファイルの改ざん検知をおこない、記憶部から読み出した複製対象となるコンテンツファイル、版管理情報および属性情報を複製先に複製し、複製された属性情報に含まれる属性コードを謄本を示す属性コードに変更し、変更された属性コードを含む属性情報および暗号鍵を用いて第3の改ざん検知情報を再算定し、再算定された第3の改ざん検知情報を含むエントリによりデータリストを更新し、更新後のデータリストに係る第4の改ざん検知情報を暗号鍵を用いて再算定するよう構成したので、電子データが複数のコンテンツファイルからなる場合であっても、版を指定した複製を効率良くおこなうことができる原本性保証電子保存方法が得られるという効果を奏する。

【0239】また、請求項15の発明に係る記録媒体は、請求項8～14のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項8～14の動作をコンピュータによって実現することができる。

【図面の簡単な説明】

【図1】この実施の形態で用いる原本性保証電子保存装置の構成を示すブロック図である。

【図2】図1に示した大容量記憶媒体に保存する保存データのデータ構造の一例を示す説明図である。

【図3】図1に示した原本性保証電子保存装置による新規データの保存処理手順を示すフローチャートである。

【図4】図3に示したバージョン属性情報の作成処理手順を示すフローチャートである。

【図5】図4に示したコンテンツ属性情報の作成処理手順を示すフローチャートである。

【図6】図3に示したデータ属性情報の作成処理手順を示すフローチャートである。

【図7】図3に示した保存データリストエントリの追加処理手順を示すフローチャートである。

【図8】図3～図7において説明した新規データの保存処理の一例を示す説明図である。

【図9】図1に示した大容量記憶媒体のマウント処理手順を示すフローチャートである。

【図10】図1に示した原本性保証電子保存装置による

データ読み出し処理手順を示すフローチャート（その1）である。

【図11】図1に示した原本性保証電子保存装置によるデータ読み出し処理手順を示すフローチャート（その2）である。

【図12】図1に示した原本性保証電子保存装置による謄本作成処理手順を示すフローチャート（その1）である。

【図13】図1に示した原本性保証電子保存装置による謄本作成処理手順を示すフローチャート（その2）である。

【図14】図1に示した原本性保証電子保存装置による謄本作成処理手順を示すフローチャート（その3）である。

【図15】図1に示した原本性保証電子保存装置による謄本作成処理手順を示すフローチャート（その4）である。

【図16】図1に示した原本性保証電子保存装置のデータ移動処理手順を示すフローチャート（その1）である。

【図17】図1に示した原本性保証電子保存装置のデータ移動処理手順を示すフローチャート（その2）である。

【図18】図13に示した保存データリストエントリの削除処理手順を示すフローチャートである。

【図19】異なる原本性保証電子保存装置にデータ移動処理をおこなう場合の移動先の原本性保証電子保存装置における転送受け入れ処理手順を示すフローチャート（その1）である。

【図20】異なる原本性保証電子保存装置にデータ移動処理をおこなう場合の移動先の原本性保証電子保存装置における転送受け入れ処理手順を示すフローチャート（その2）である。

【図21】図1に示した原本性保証電子保存装置によるデータの削除処理手順を示すフローチャートである。

【図22】図1に示した原本性保証電子保存装置によるデータ属性コードの変更態様を示す説明図である。

【図23】図1に示した原本性保証電子保存装置によるデータ属性コードの変更処理手順を示すフローチャート（その1）である。

【図24】図1に示した原本性保証電子保存装置によるデータ属性コードの変更処理手順を示すフローチャート（その2）である。

【図25】図24に示した保存データリストエントリの更新処理手順を示すフローチャートである。

【図26】図1に示した原本性保証電子保存装置によるデータのバージョンアップ処理手順を示すフローチャートである。

【図27】図1に示した原本性保証電子保存装置によるデータの編集処理手順を示すフローチャートである。

49

【図 2 8】 図 1 に示した原本性保証電子保存装置へのクライアントからのログイン処理手順を示すフローチャートである。

【図 2 9】 図 1 に示した原本性保証電子保存装置が用いるタイマ設定履歴およびアクセス履歴の一例を示す図である。

【図 3 0】 図 1 に示した原本性保証電子保存装置が用いる保存データリストファイルおよびデータ属性情報ファイルの一例を示す図である。

【図 3 1】 図 1 に示した原本性保証電子保存装置が用いるバージョン属性情報、コンテンツ属性情報および媒体認証リストコードの一例を示す図である。

50

【図 3 2】 図 1 に示した原本性保証電子保存装置が用いるアカウント管リスト、日時情報およびタイマ設定履歴ファイルの一例を示す説明図である。

【符号の説明】

1 0 0 原本性保証電子保存装置

1 0 1 大容量記憶媒体

1 0 2 通信ポート

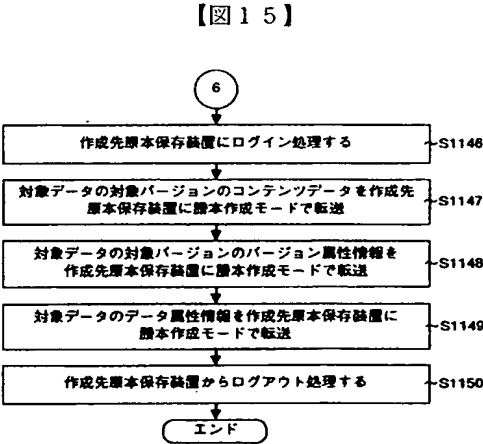
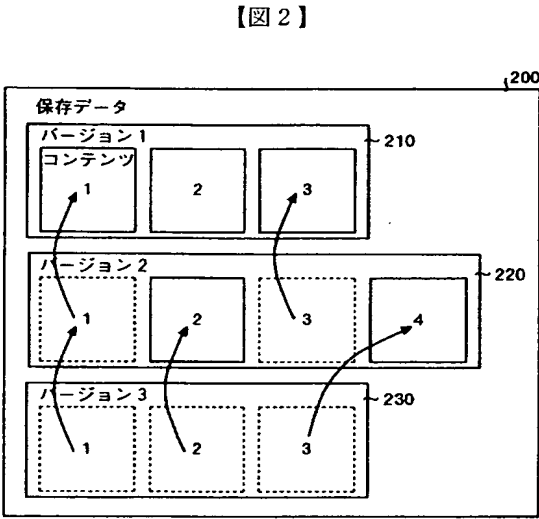
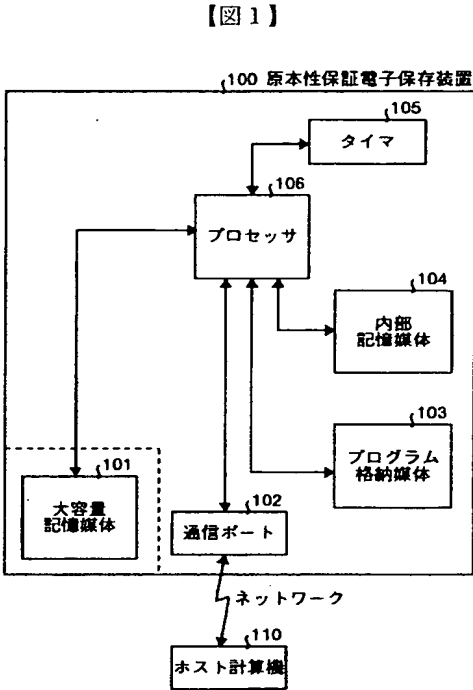
1 0 3 プログラム格納媒体

1 0 4 内部記録媒体

1 0 5 タイマ

1 0 6 プロセッサ

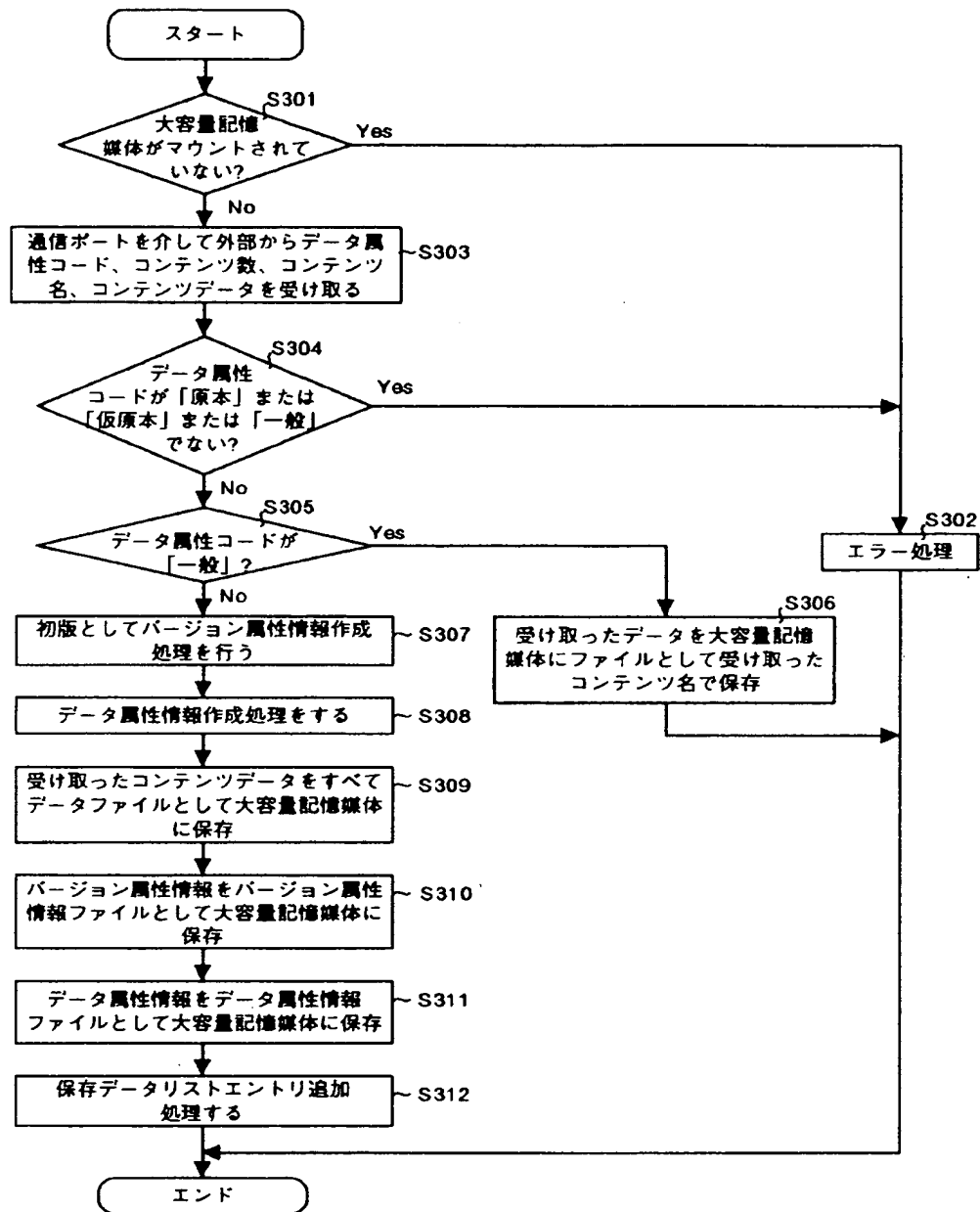
1 1 0 ホスト計算機



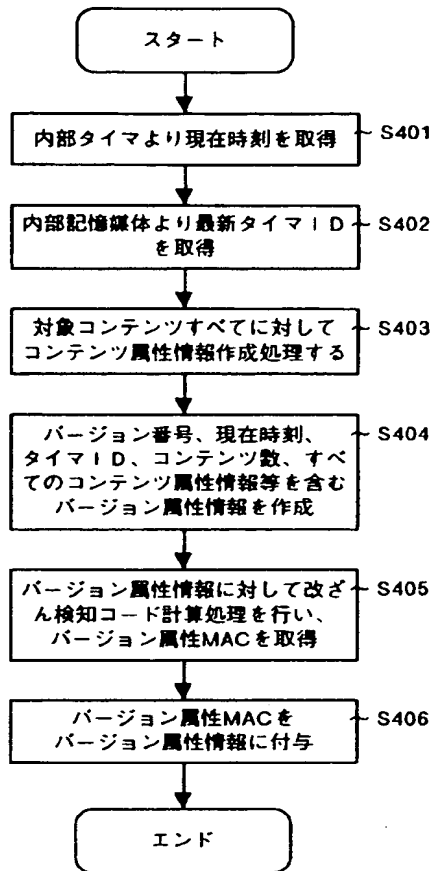
【図 2 2】

復旧前	復旧後
謄本	原本
バックアップ仮原本	仮原本
バックアップ原本	原本
バックアップ謄本	謄本

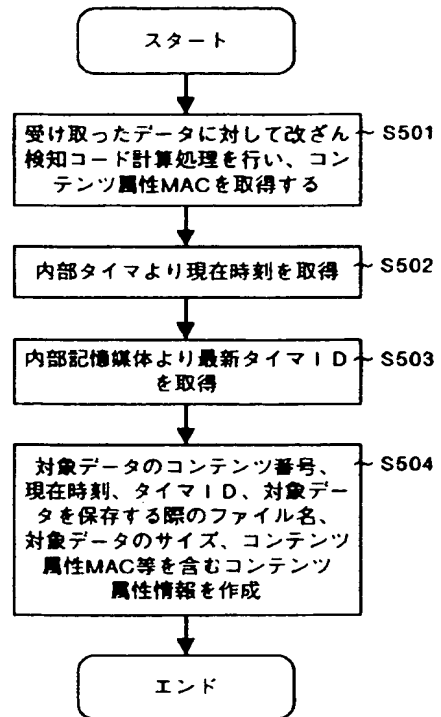
【図3】



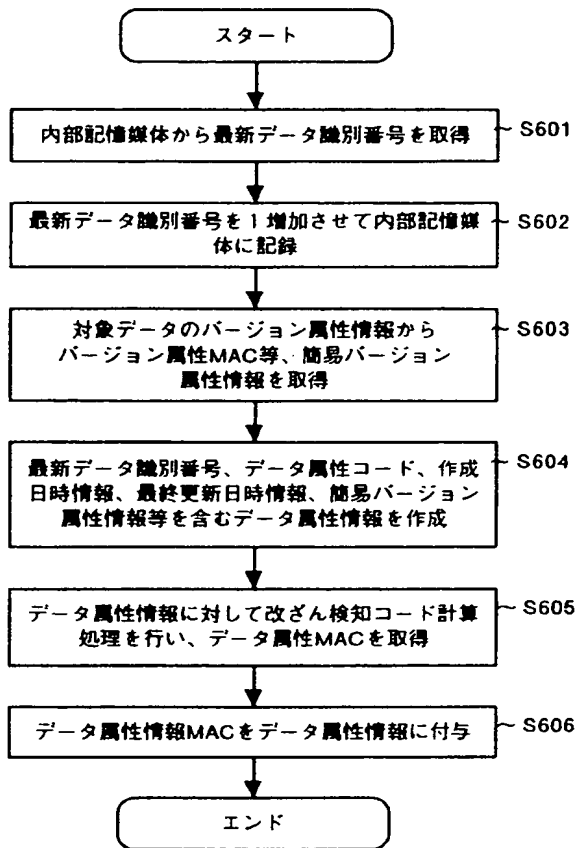
【図4】



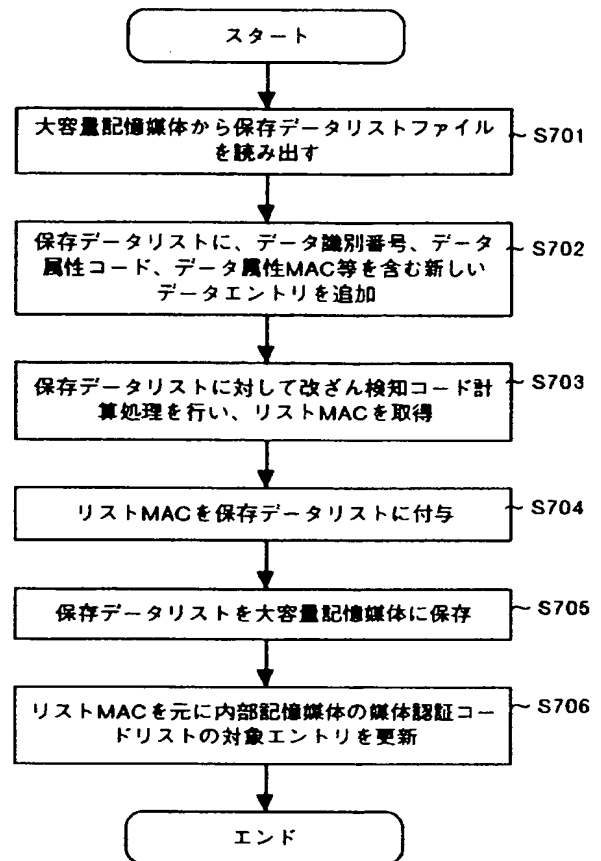
【図5】



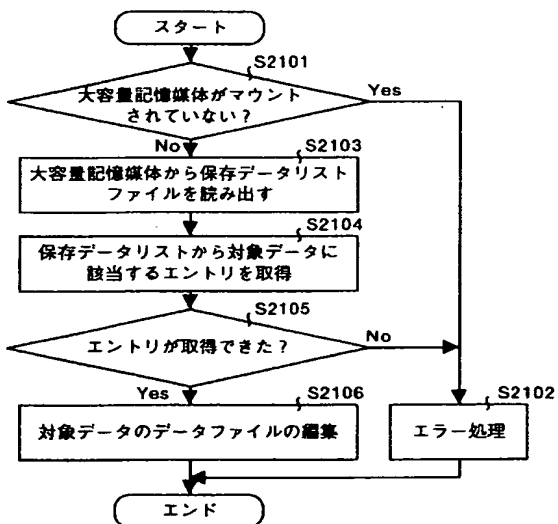
【図6】



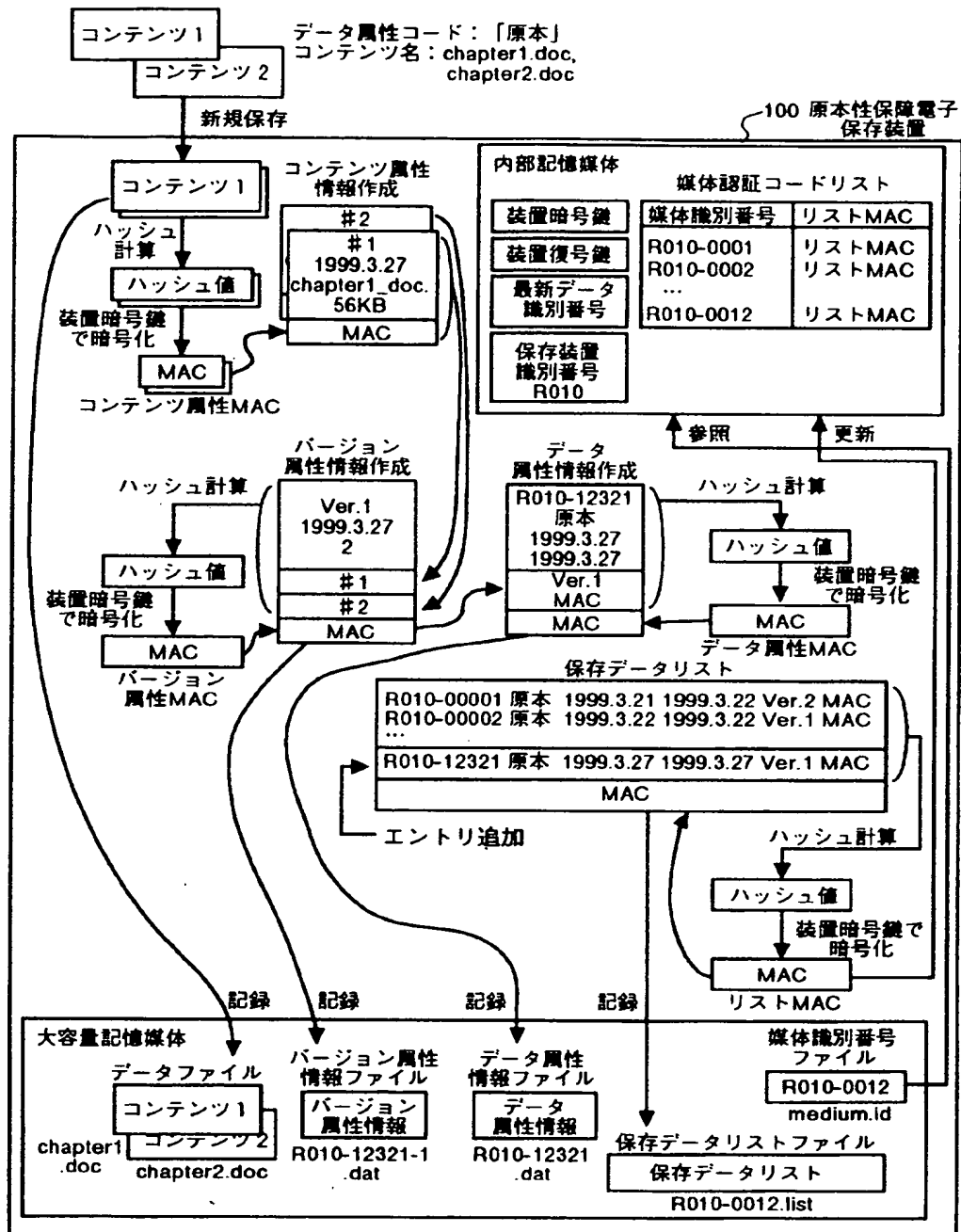
【図7】



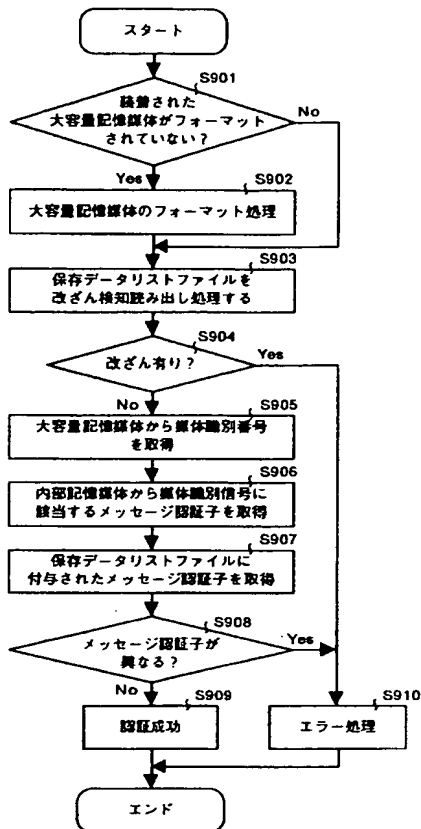
【図27】



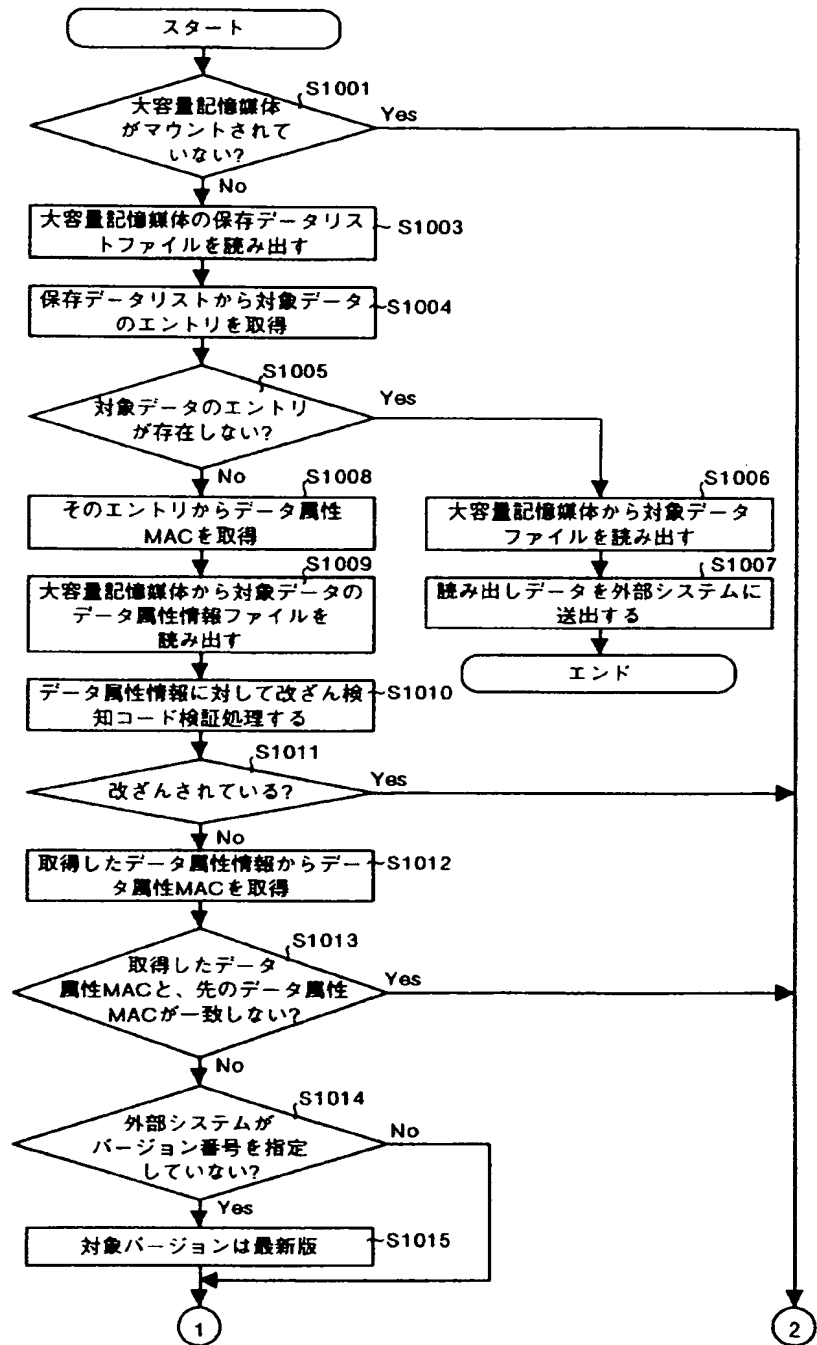
【図8】



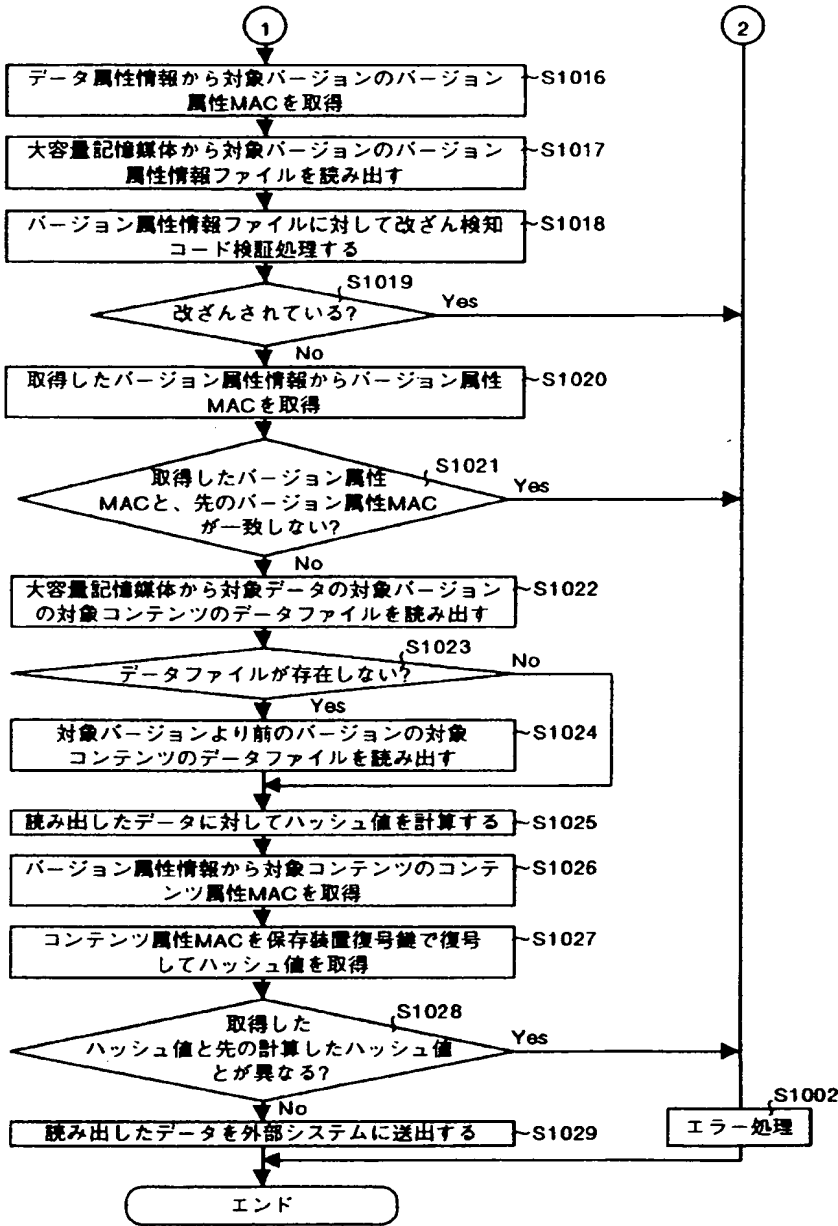
【図9】



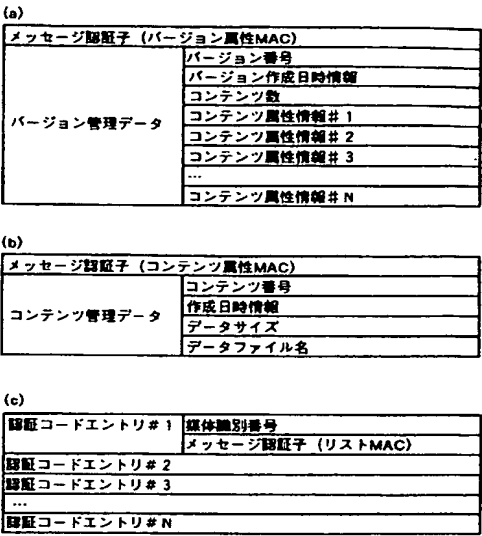
【図10】



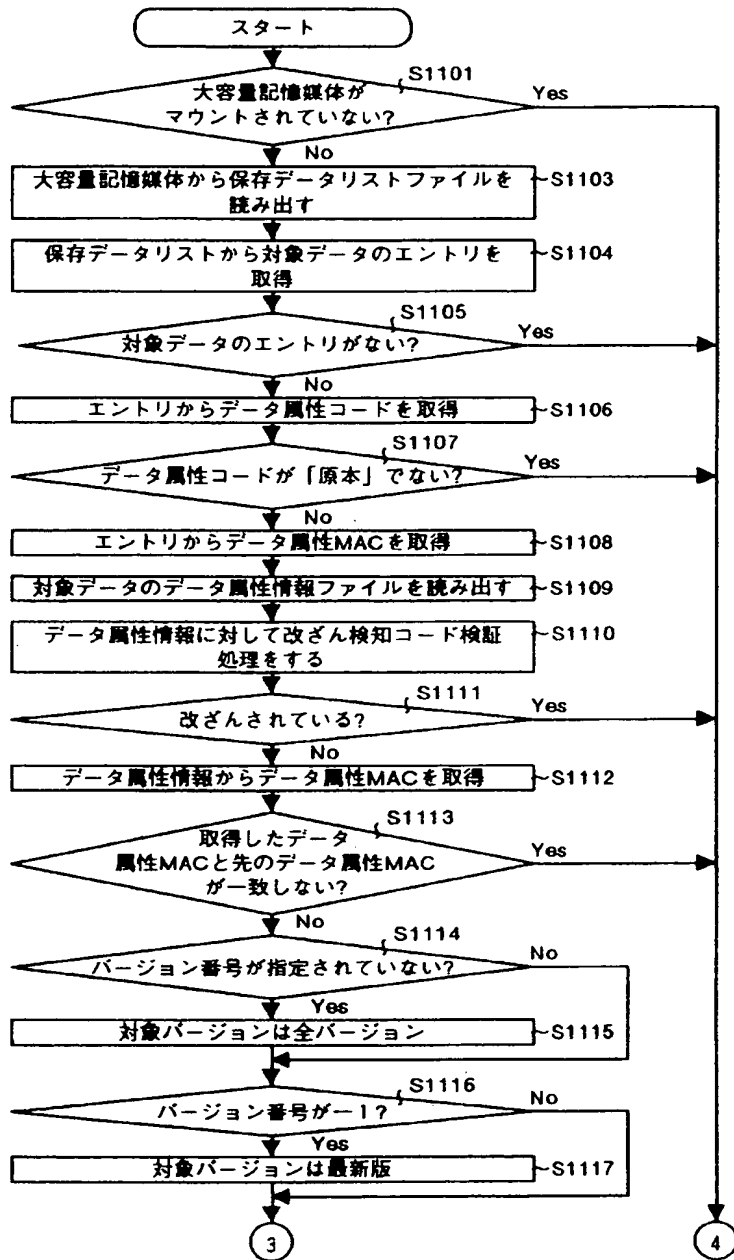
【図 11】



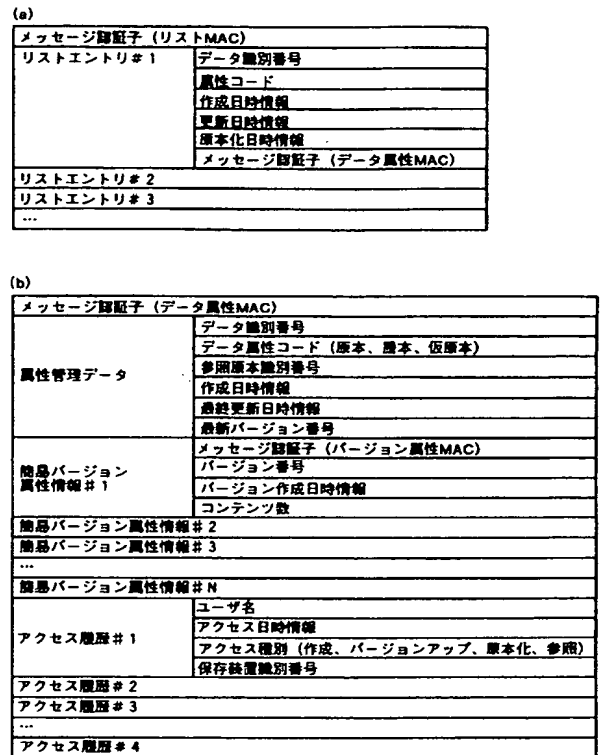
【図 31】



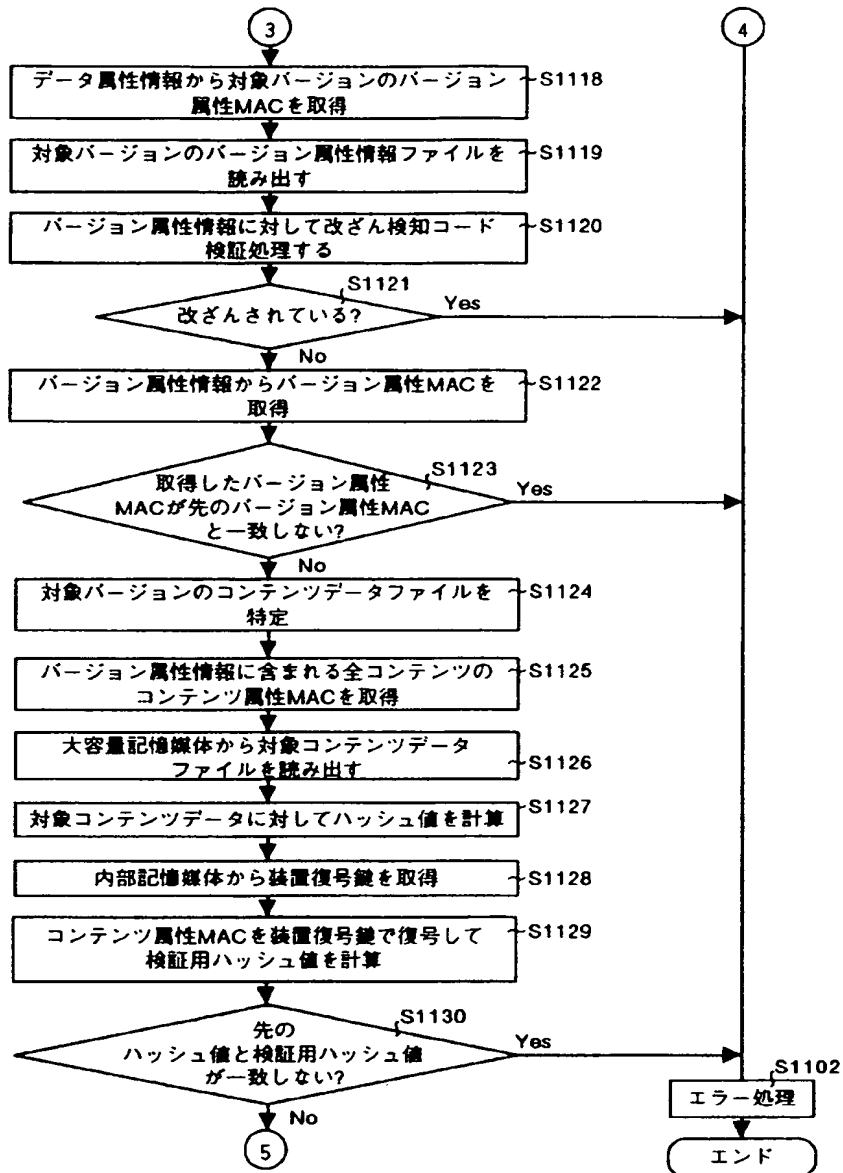
【図12】



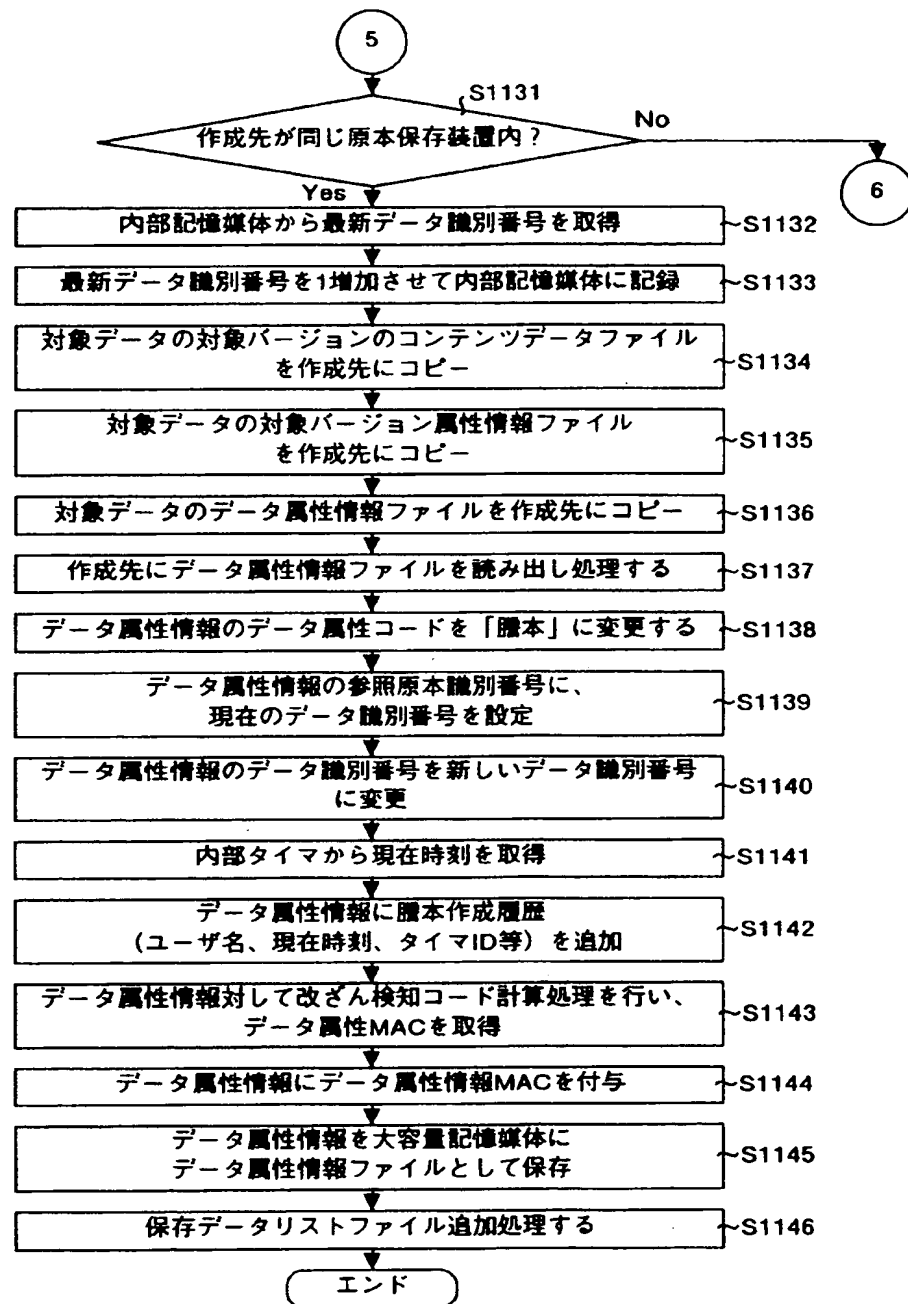
【図30】



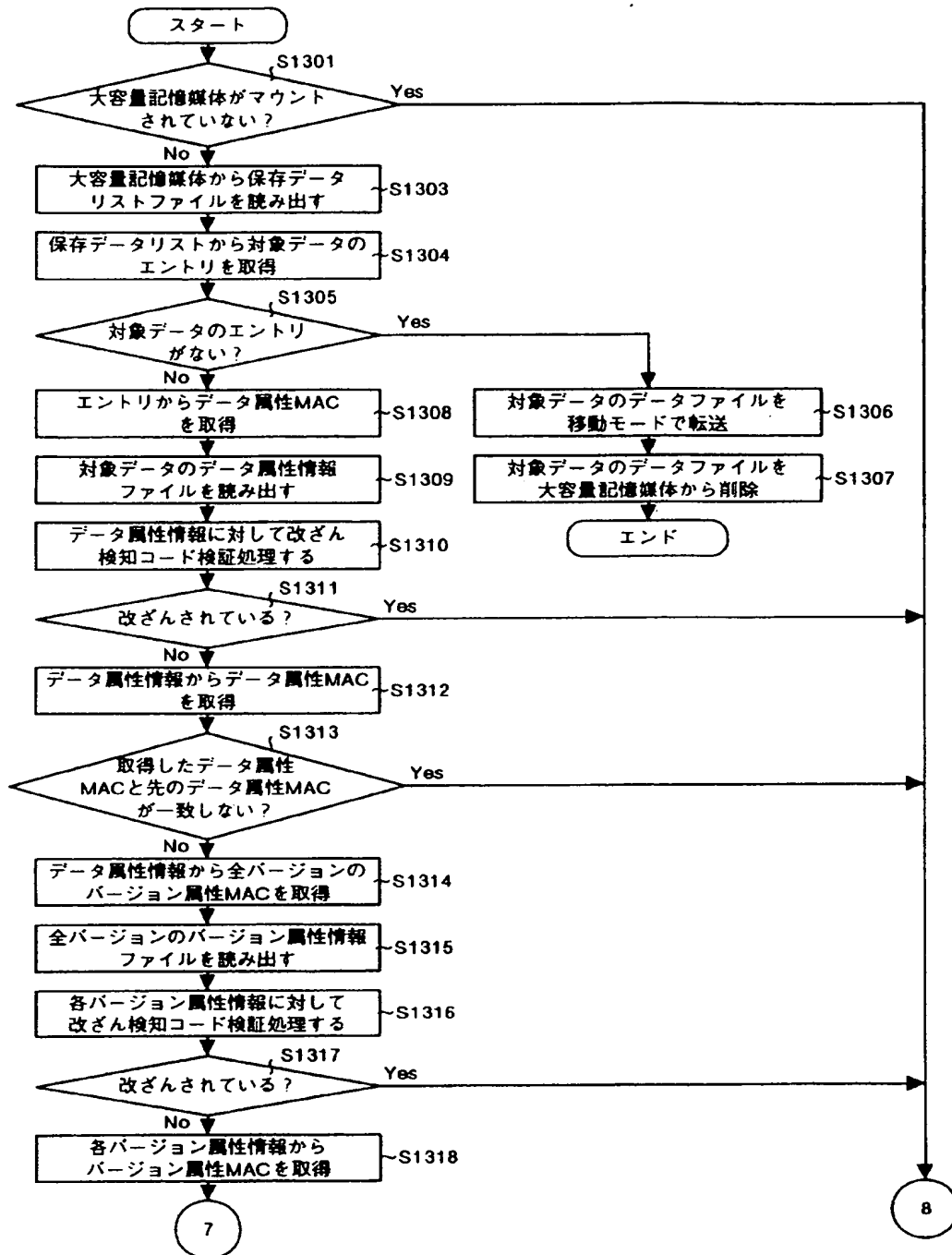
【図13】



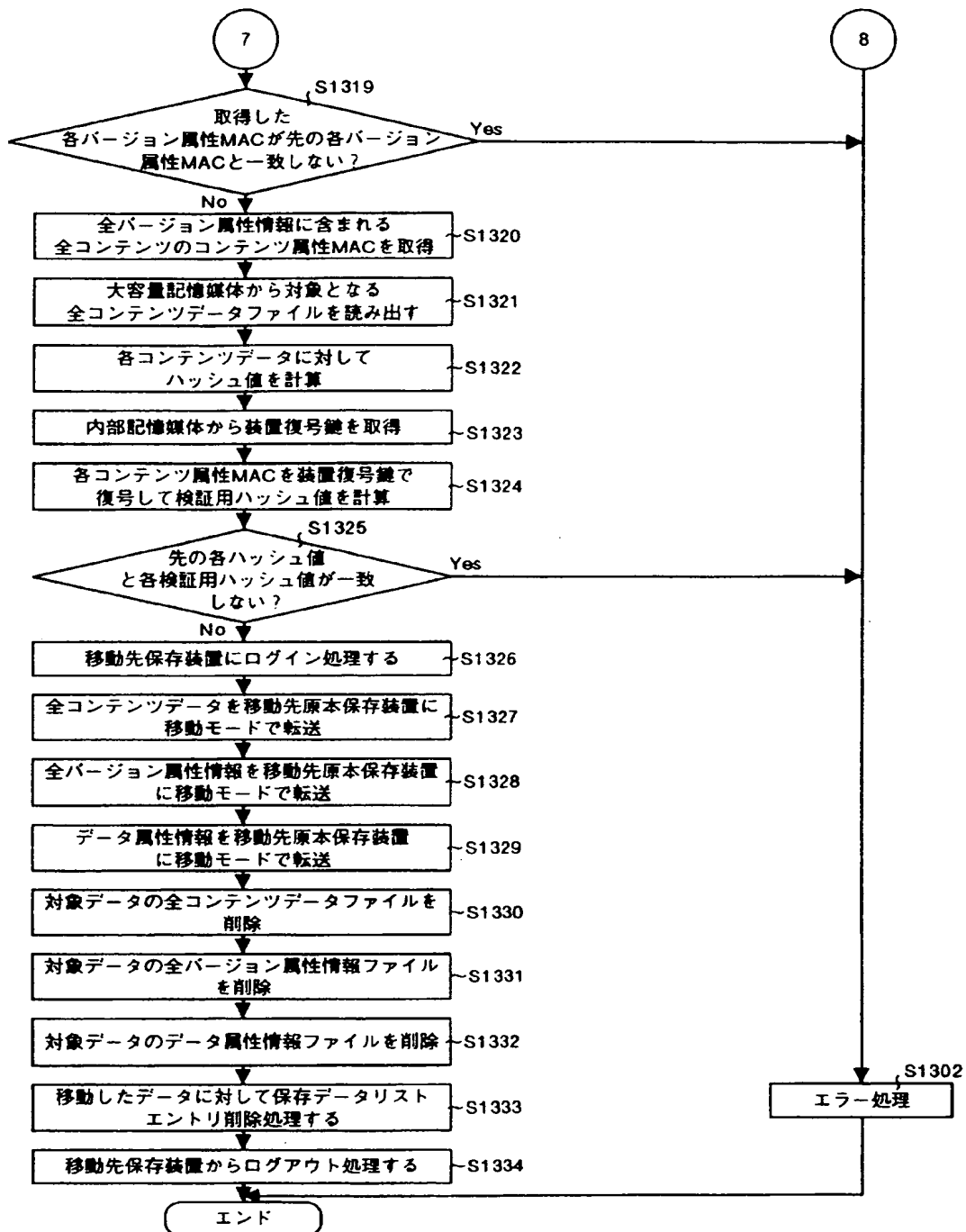
【図14】



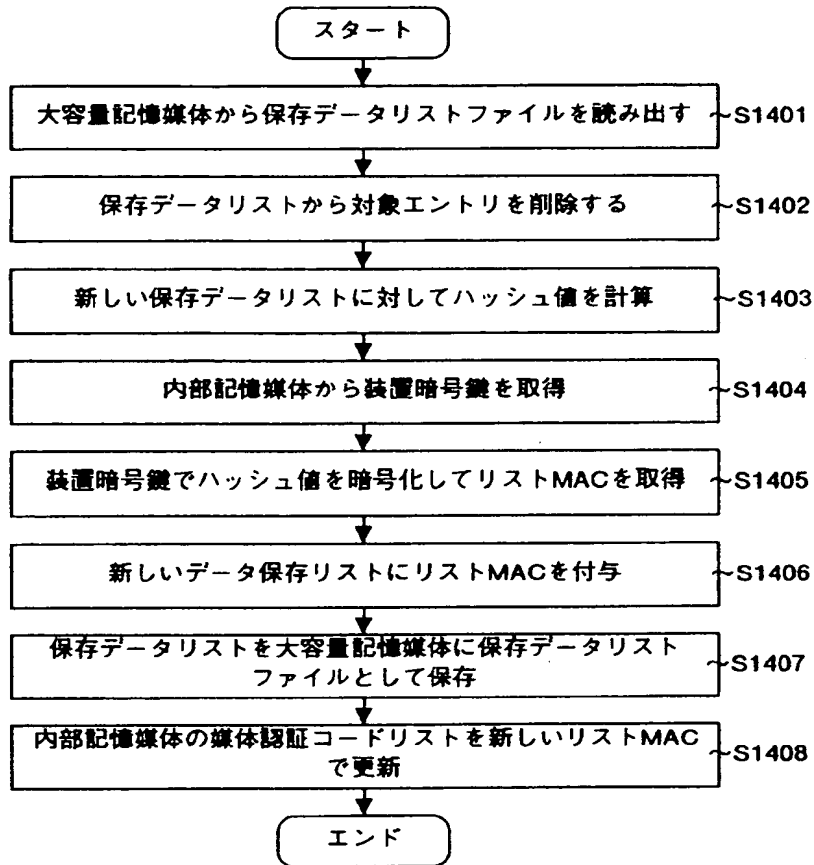
【図16】



【図17】



【図 18】



【図 29】

(a)

変更前	変更後
19990215 15:32:14 ID=1	19990215 15:30:00 ID=2
19990216 10:21:54 ID=2	19990116 10:22:00 ID=3
19990116 10:45:23 ID=3	19990216 10:46:00 ID=4

(b)

アクセス種別	アクセス日時	装置ID
CREATE	19990215 18:23:10 ID=1	R010-0001032
APPEND	19990215 18:23:30 ID=1	R010-0001032
MOVE TO	19990217 10:10:21 ID=3	R010-0001032
MOVE FROM	19990217 10:13:43 ID=2	R010-0001055

【図 32】

(a)

アカウントエントリ # 1	アカウント名
アカウントエントリ # 2	パスワード
アカウントエントリ # 3	
...	
アカウントエントリ # N	

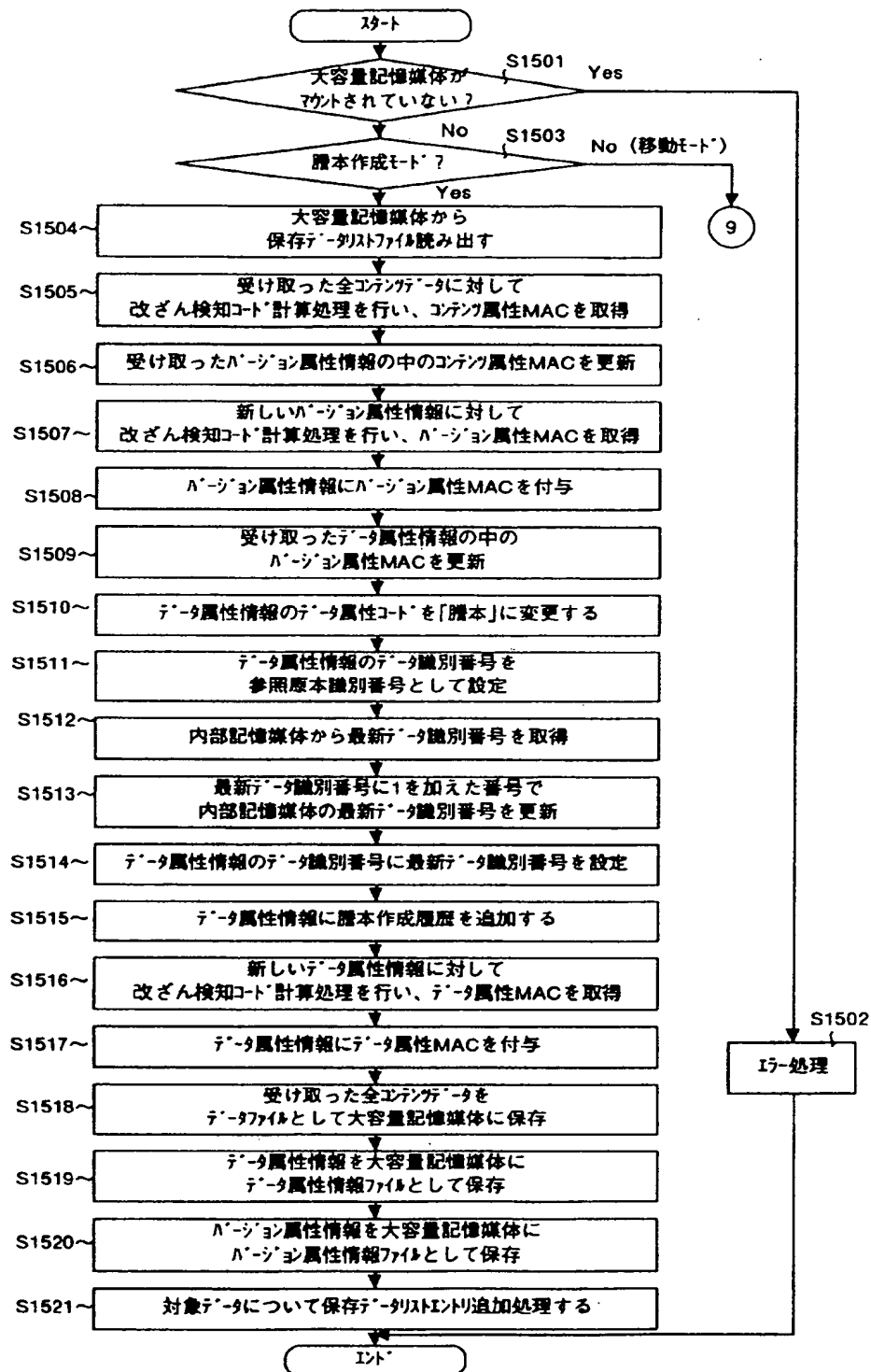
(b)

年
月
日
時
分
秒
GST (世界標準時) からのずれ
タイムID

(c)

タイム設定履歴 # 1	設定前の日時情報
	設定後の日時情報
タイム設定履歴 # 2	アカウント名
タイム設定履歴 # 3	
...	
タイム設定履歴 # N	

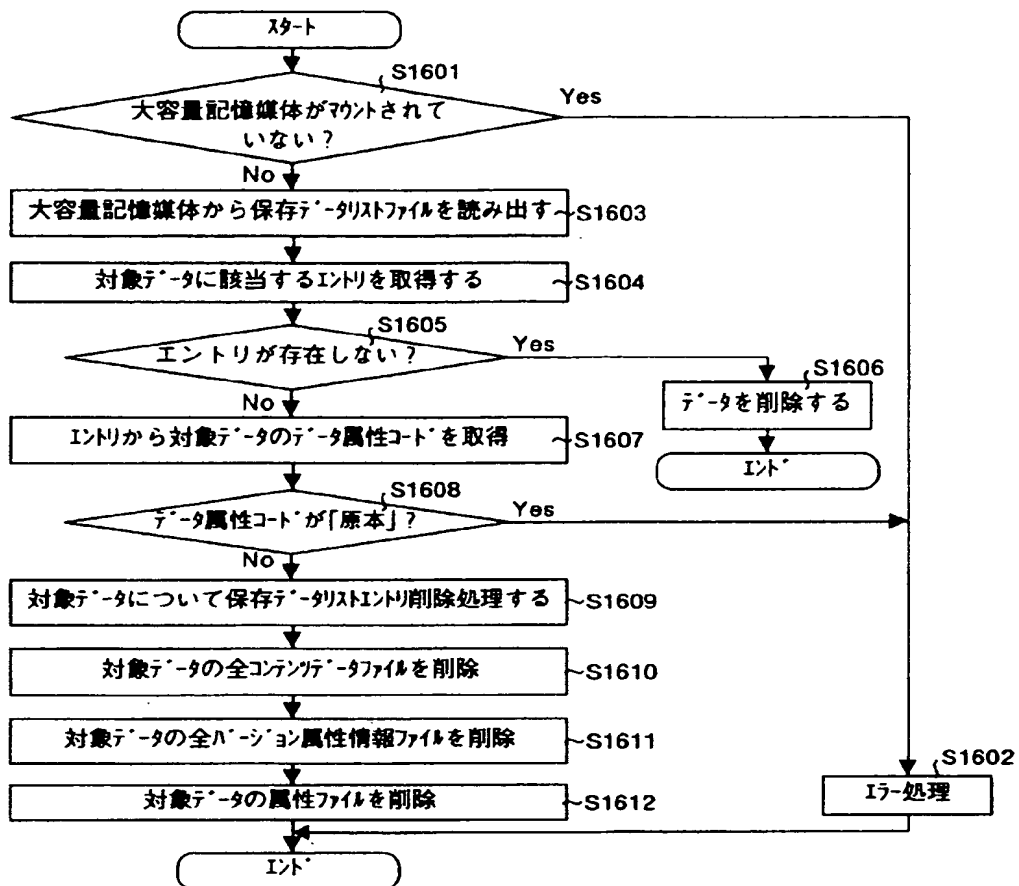
【図19】



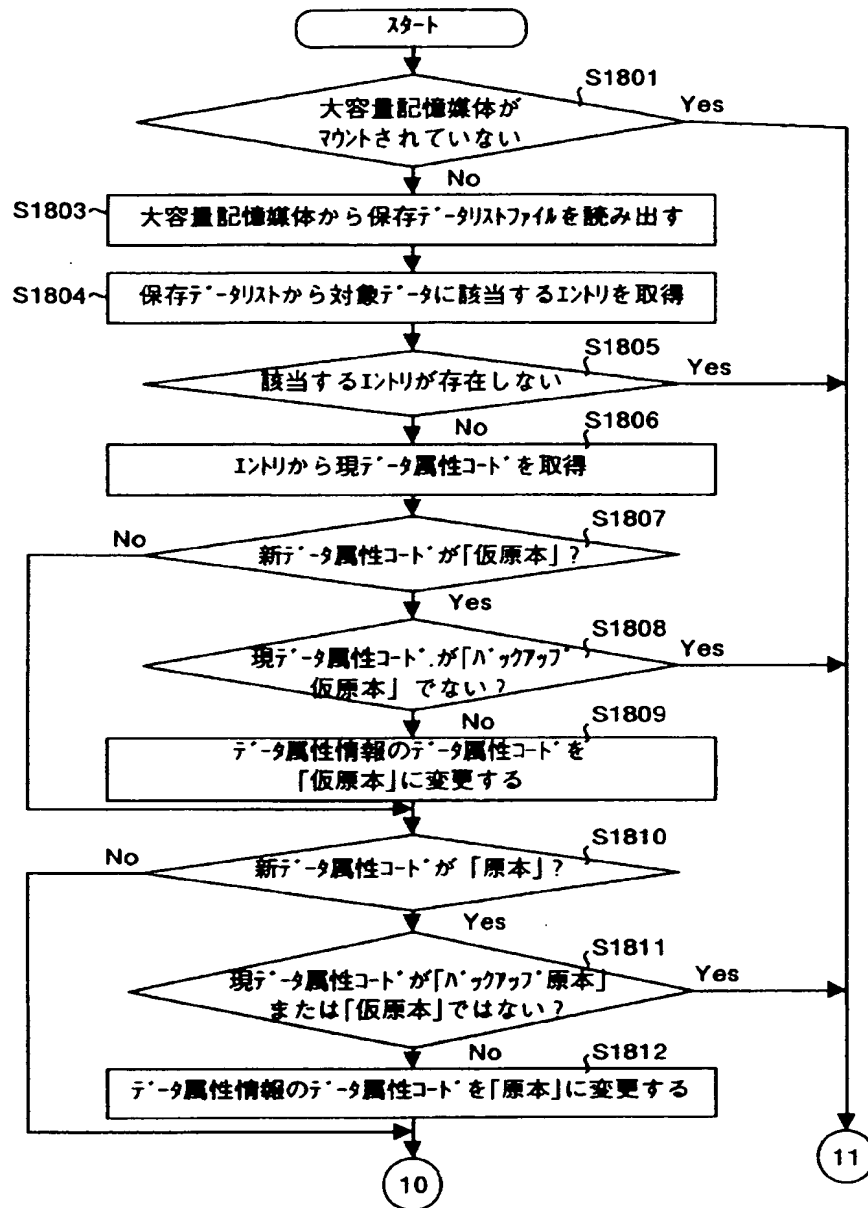
【図20】



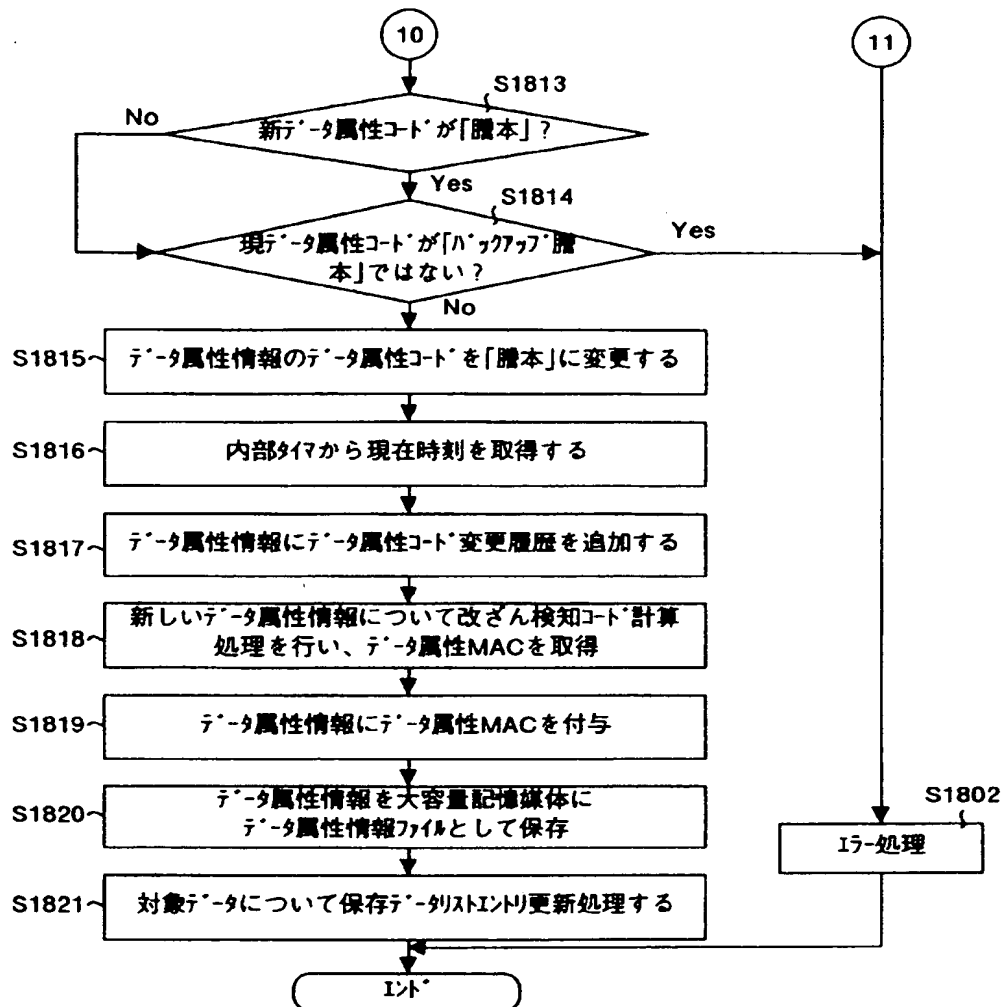
【図21】



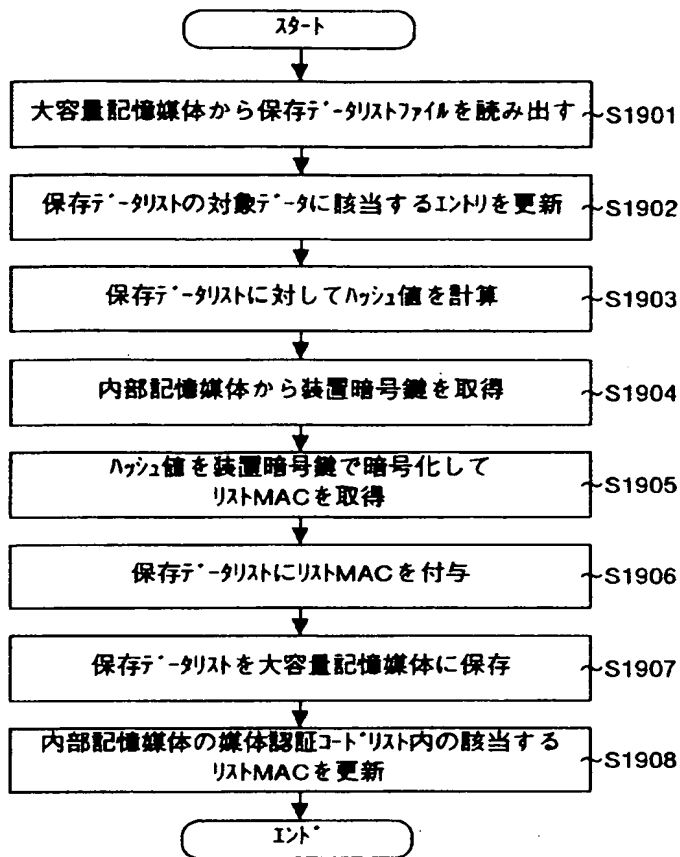
【図23】



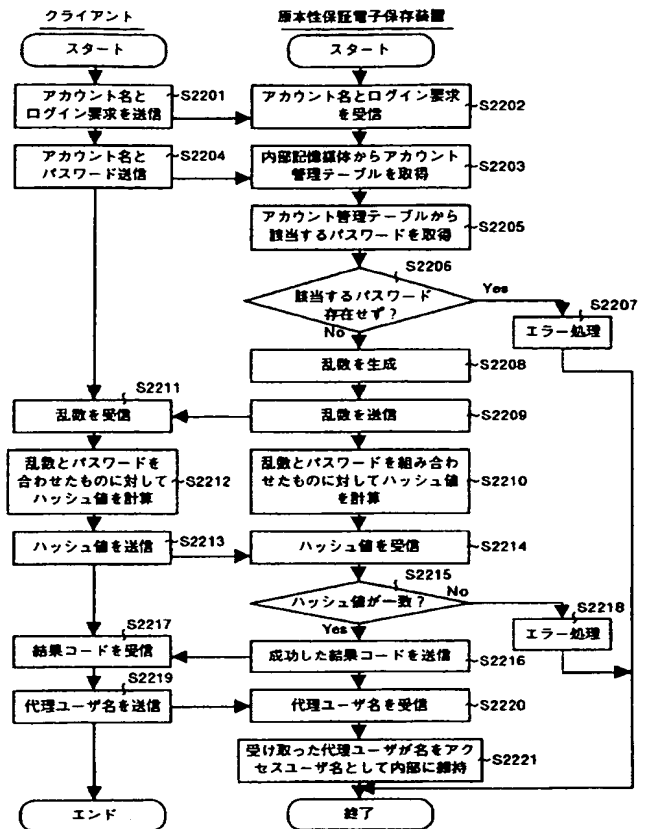
【図24】



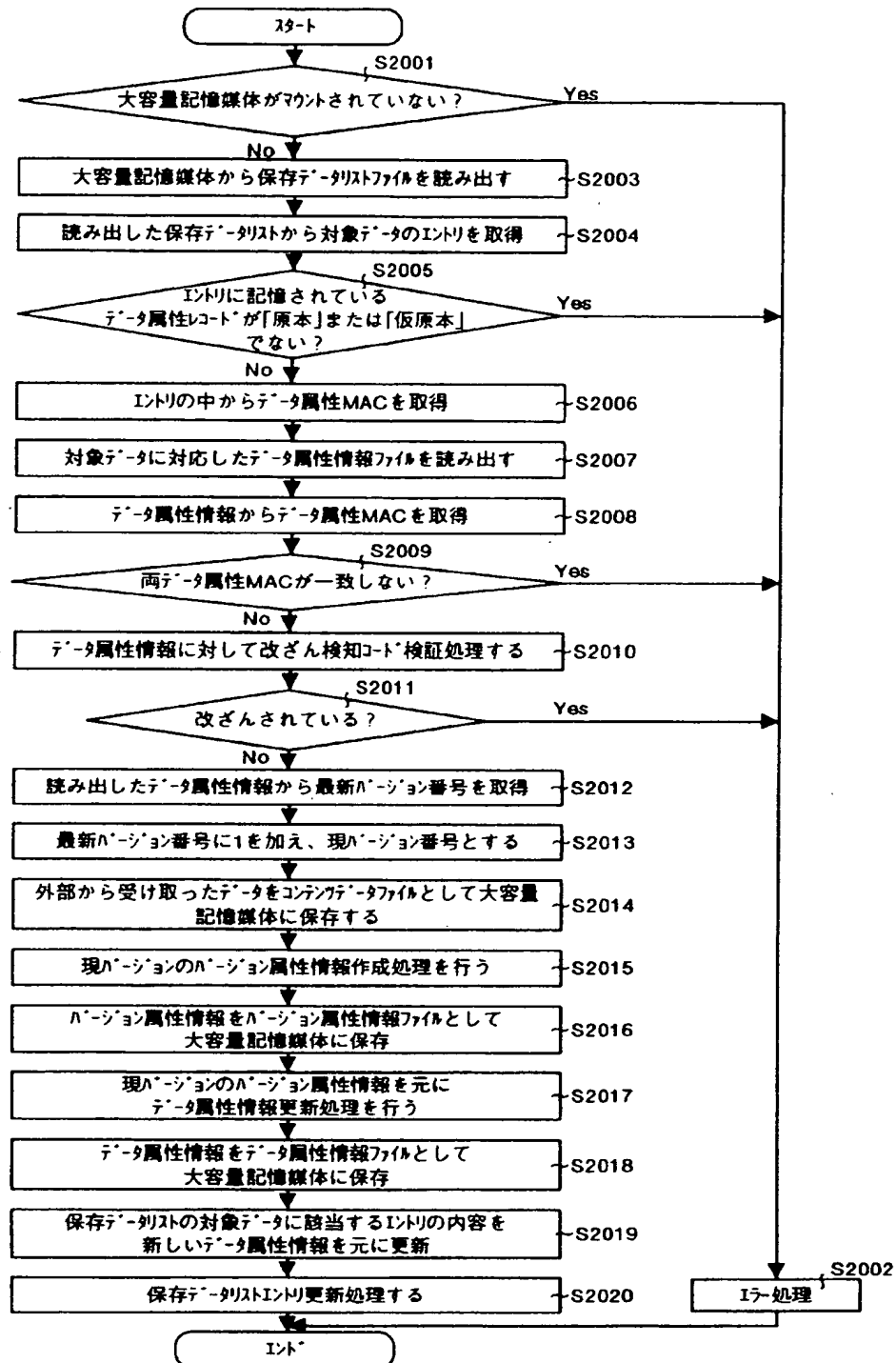
【図 25】



【図 28】



【図26】



フロントページの続き

(51) Int. Cl.⁷

識別記号

F I

テーマコード(参考)

G 0 6 F 15/401

3 4 0 B

F ターム(参考) 5B017 AA02 BA02 BB06 CA16
5B049 CC00 EE05 GG02 GG10
5B075 KK54 NR20 NS10 OS01 UU06
5B082 AA00 DD08 EA01 EA07 EA11
GA05 GA11 GA20